Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) om meddelelsen fra Kommissionen til Europa-Parlamentet og Rådet om et område med frihed, sikkerhed og retfærdighed i borgernes tjeneste

(2009/C 276/02)

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,

som henviser til 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, særlig artikel 41,

HAR VEDTAGET FØLGENDE UDTALELSE:

I. INDLEDNING

1. Den 10. juni 2009 vedtog Kommissionen sin meddelelse til Europa-Parlamentet og Rådet om et område med frihed, sikkerhed og retfærdighed i borgernes tjeneste ([1]). I overensstemmelse med artikel 41 i forordning (EF) nr. 45/2001 forelægger EDPS hermed sin udtalelse.

2. Kommissionen havde inden vedtagelsen af meddelelsen ved skrivelse af 19. maj 2009 uformelt hørt EDPS derom. EDPS svarede på denne høring den 20. maj 2009 ved at fremsende uformelle bemærkninger med det formål yderligere at forbedre meddelelsesteksten. Endvidere har EDPS aktivt bidraget til skrivelsen af 14. januar 2009 fra Gruppen vedrørende Politi og Retsvæsen om det flerårige program for området med frihed, sikkerhed og retfærdighed ([2]).

3. I meddelelsen (punkt 1) fremhæves det, at »EU bør have et nyt flerårigt program, der ved at bygge på de fremskridt, der er sket, og drage lære af de nuværende svagheder går fremtiden i møde med en række ambitiøse mål. Dette nye program bør foretage en prioritering for de næste fem år«. Dette flerårige program (allerede kendt som »Stockholmprogrammet«) vil være opfølgningen af Tammerfors- og Haagprogrammerne, der politisk udgjorde en vigtig tilskyndelse til området med frihed, sikkerhed og retfærdighed.

4. Det er meningen, at meddelelsen skal danne grundlag for dette nye flerårige program. EDPS noterer sig i denne forbindelse, at selv om de flerårige programmer ikke i sig selv er bindende instrumenter, har de en betydelig indvirkning på den politik, som institutionerne vil udvikle på det pågældende område, da mange af de konkrete lovgivningsmæssige og ikke-lovgivningsmæssige tiltag vil være en følge af programmet.

5. Meddelelsen skal ses i dette perspektiv. Den udgør næste skridt i en debat, der mere eller mindre begyndte med to rapporter, der blev forelagt i juni 2008 af den såkaldte »Fremtidsgruppe« nedsat af formandskabet for Rådet for at udforme idéer: »Frihed, sikkerhed, privatlivets fred — europæiske indre anliggender i en åben verden« ([3]) og »Foreslåede løsninger for det fremtidige EU-program for retlige anliggender« ([4]).

II. UDTALELSENS HOVEDINDHOLD

6. Den foreliggende udtalelse er ikke kun en reaktion på meddelelsen, men den er også et bidrag fra EDPS til den mere generelle debat om fremtiden for området med frihed, sikkerhed og retfærdighed, der skal udmøntes i et nyt strategisk arbejdsprogram (Stockholmprogrammet) som bebudet af det svenske formandskab for EU ([5]). Denne udtalelse vil også behandle nogle af følgerne af Lissabon-traktatens eventuelle ikrafttræden.

7. Efter en præcisering af udtalelsens væsentligste perspektiver i del III gives der en generel vurdering af meddelelsen i del IV.

8. I del V behandles spørgsmålet om, hvordan man kan tilgodese behovet for fortsat beskyttelse af privatlivets fred og personoplysninger i en kontekst af stigende udveksling af personoplysninger. Der sættes fokus på meddelelsens punkt 2.3 vedrørende beskyttelse af personoplysninger og af privatlivets fred og mere generelt på behovet for supplerende tiltag, eventuelt i form af retsakter, for at forbedre rammen for databeskyttelse.

([1]) KOM(2009) 262 endelig (»meddelelsen«).

([2]) Ikke offentliggjort. Gruppen vedrørende Politi og Retsvæsen (WPPJ) blev oprettet af den europæiske konference for datatilsynsmyndigheder med henblik på at udarbejde holdninger på området retshåndhævelse og handle på dens vegne i hastesager.

([3]) Rådets dok. nr. 11657/08. I det følgende benævnt »rapporten om indre anliggender«.

([4]) Rådets dok. nr. 11549/08 (i det følgende benævnt »rapporten om retlige anliggender«).

([5]) Regeringernes EU-arbejdsprogram, http://www.regeringen.se

9. I del VI drøftes behovene og mulighederne for lagring af, adgang til og udveksling af oplysninger som instrumenter til retshåndhævelse eller, som det hedder i meddelelsen, til »et Europa, der beskytter«. Punkt 4 i meddelelsen indeholder en række mål vedrørende informa-tion og teknologiske værktøjer, især punkt 4.1.2 (Udnyttelse af informationen), 4.1.3 (Mobilisering af de nødvendige teknologiske værktøjer) og 4.2.3.2 (Informationssystemerne). Udviklingen af en europæisk informationsmodel (i punkt 4.1.2) kan ses som det mest udfordrende forslag i denne forbindelse. EDPS's udtalelse analyserer dette forslag grundigt.

10. Del VII berører kort et bestemt emne inden for områderne frihed, sikkerhed og retfærdighed, der er relevante for databeskyttelse, nemlig adgang til retlig prøvelse og e-justice.

III. UDTALELSENS PERSPEKTIVER

11. I denne udtalelse er behovet for beskyttelse af de grundlæggende rettigheder hovedvinklen i analysen af meddelelsen og mere generelt fremtiden for området med frihed, sikkerhed og retfærdighed, som udformet i et nyt flerårigt program. Den vil endvidere basere sig på bidragene fra EDPS til udviklingen af EU's politik på dette område, hovedsagelig i dennes høringsrolle. EDPS har indtil videre vedtaget mere end 30 udtalelser og bemærkninger om initiativer, der stammer fra Haagprogrammet, og som alle kan findes på den tilsynsførendes websted.

12. EDPS vil i sin vurdering af meddelelsen især tage hensyn til følgende fire perspektiver, som er relevante for fremtiden for området med frihed, sikkerhed og retfærdighed. Alle disse perspektiver spiller også en central rolle i meddelelsen.

13. Det første perspektiv er den eksponentielle vækst i digital information om borgerne som følge af informations- og kommunikationsteknologier, der er under stadig udvikling ([6]). Samfundet bevæger sig i retning af, hvad der ofte kaldes »et overvågningssamfund«, hvor enhver transaktion og næsten enhver af borgernes bevægelser kan forventes at blive registreret digitalt. De såkaldte »tingenes internet« og »intelligente omgivelser« er allerede under hastig udvikling via anvendelsen af RFID-brikker. Menneskekroppens digitaliserede karakteristika (biometriske identifikatorer) anvendes i stadig større grad. Dette fører til en til stadighed mere forbundet verden, hvor de offentlige sikkerhedsorganisationer kan få adgang til umådeligt store mængder potentielt nyttige oplysninger, der direkte kan påvirke de pågældende personers liv.

14. Det andet perspektiv er internationalisering. På den ene side er dataudveksling i den digitale tidsalder ikke begrænset af Den Europæiske Unions eksterne grænser, mens der på den anden side er et stadigt stigende behov for internationalt samarbejde inden for alle EU's aktiviteter på området med frihed, sikkerhed og retfærdighed: bekæmpelse af terrorisme, politisamarbejde og retligt samarbejde, civilret og grænsekontrol er blot nogle eksempler.

15. Det tredje perspektiv er anvendelse af data til retshåndhævelsesformål: den seneste tids trusler mod samfundet, uanset om de har været terrorismerelaterede eller ej, har ført til (krav om), at de retshåndhævende myndigheder får flere muligheder for at indsamle, lagre og udveksle personoplysninger. I mange tilfælde er private aktivt involveret, som det blandt andet fremgår af direktivet om lagring af data ([7]) og de forskellige instrumenter vedrørende PNR ([8]).

16. Det fjerde perspektiv er fri bevægelighed. Den gradvise udvikling af et område med frihed, sikkerhed og retfærdighed gør det nødvendigt, at interne grænser og eventuelle hindringer for den frie bevægelighed inden for området i endnu højere grad. Nye instrumenter på dette område bør under alle omstændigheder ikke genindføre hindringer. Fri bevægelighed omfatter i den aktuelle kontekst dels fri bevægelighed for personer og dels fri bevægelighed for (person)oplysninger.

17. Disse fire perspektiver viser, at den kontekst, hvori oplysninger anvendes, er under hastig forandring. I en sådan kontekst kan der ikke være tvivl om betydningen af en stærk mekanisme til beskyttelse af borgernes grundlæggende rettigheder og især beskyttelse af privatlivets fred og databeskyttelse. Af disse grunde vælger EDPS behovet for beskyttelse som hovedvinklen for sin analyse som nævnt i punkt 11.

([6]) Rapporten om indre anliggender taler i denne forbindelse endda om en »digital tsunami«.

([7]) Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (EUT L 105 af 13.4.2006, s. 54).

([8]) Jf. f.eks. aftalen mellem Den Europæiske Union og Amerikas Forenede Stater om luftfartsselskabers behandling og overførsel af passagerliste (PNR)-oplysninger til United States Department of Homeland Security (DHS) (PNR-aftale 2007) (EUT L 204 af 4.8.2007, s. 18) og forslag til Rådets rammeafgørelse om anvendelse af passagerlister (PNR-oplysninger) med henblik på retshåndhævelse, KOM(2007) 654 endelig.

IV. GENEREL VURDERING

18. Det er formålet med meddelelsen og Stockholmprogrammet at præcisere EU's hensigter for de kommende fem år, eventuelt med virkninger på endnu længere sigt. EDPS noterer sig, at meddelelsen er udfærdiget på en såkaldt »Lissabonneutral« måde. EDPS forstår fuldt ud, hvorfor Kommissionen har anvendt denne tilgang, men beklager, at meddelelsen ikke fuldt ud kan udnytte de yderligere fordele, som Lissabontraktaten tilbyder. Der vil i denne udtalelse blive lagt mere vægt på mulighederne i forbindelse med Lissabontraktaten.

19. Meddelelsen bygger på resultaterne af EU's tiltag inden for området med frihed, sikkerhed og retfærdighed i de seneste år. Disse resultater kan karakteriseres som hændelsesstyrede med vægt på foranstaltninger, der udvider retshåndhævelsesmyndighedernes beføjelser, og som er indgribende over for borgerne. Det er i særdeleshed tilfældet for de områder, hvor personoplysninger i vid udstrækning anvendes og udveksles, og som derfor er af afgørende betydning for databeskyttelse. Resultaterne er hændelsesstyrede, eftersom eksterne hændelser, såsom 11. september og bombeattentaterne i Madrid og London, gav en vigtig tilskyndelse til lovgivningsmæssige aktiviteter. For eksempel kan overførslen af oplysninger om passagerer til USA betragtes som en følge af 11. september ([9]), mens bombeattentaterne i London førte til direktiv 2006/24/EF om lagring af data ([10]). Der blev lagt vægt på mere indgribende foranstaltninger, da EU-lovgiveren fokuserede på foranstaltninger, der letter anvendelsen og udvekslingen af data, mens drøftelserne om foranstaltninger, der tager sigte på at sikre beskyttelsen af personoplysninger, var mindre presserende. Den væsentligste beskyttende foranstaltning, der blev vedtaget efter tre års drøftelser i Rådet, er Rådets rammeafgørelse 2008/977/RIA om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager ([11]). Resultatet var Rådets rammeafgørelse, der ikke er fuldt tilfredsstillende (jf. punkt 29-30).

20. Erfaringerne i de seneste år viser, at der er behov for at overveje følgerne for de retshåndhævende myndigheder og for de europæiske borgere, inden der vedtages nye instrumenter. Disse overvejelser bør tage behørigt hensyn til omkostningerne for privatlivets fred og effektiviteten af retshåndhævelsen, for det første når der foreslås og drøftes nye instrumenter, men også efter at disse instrumenter er gennemført, ved hjælp af regelmæssige evalueringer. Sådanne overvejelser er også af afgørende betydning, inden et nyt flerårigt program skal fastlægge de vigtigste initiativer for den nærmeste fremtid.

21. EDPS glæder sig over, at det i meddelelsen anerkendes, at beskyttelse af grundlæggende rettigheder, og navnlig beskyttelse af personoplysninger, er et af de centrale spørgsmål i forbindelse med fremtiden for området med frihed, sikkerhed og retfærdighed. I punkt 2 i meddelelsen karakteriseres EU som et unikt område for beskyttelse af grundlæggende rettigheder baseret på fælles værdier. Det er også positivt, at tiltrædelsen af den europæiske menneskerettighedskonvention nævnes som en prioriteret retningslinje — endda den første prioriterede retningslinje i meddelelsen. Tiltrædelse er et vigtigt skridt fremad for at sikre et harmonisk og sammenhængende system for beskyttelse af de grundlæggende rettigheder. Sidst, men ikke mindst, har databeskyttelse fået en fremtrædende plads i meddelelsen.

22. Dette fokus i meddelelsen viser, at man klart har til hensigt at sikre beskyttelsen af borgernes rettigheder og — herved — anlægger en mere afbalanceret tilgang. Regeringerne har brug for passende instrumenter til at garantere borgernes sikkerhed, men inden for vort europæiske samfund skal de fuldt ud respektere borgernes grundlæggende rettigheder. At handle i borgernes tjeneste ([12]) kræver en Europæisk Union, der værner om denne balance.

23. EDPS er af den opfattelse, at meddelelsen tager meget hensyn til behovet for denne balance, herunder behovet for at beskytte personoplysninger. Det erkendes, at der skal lægges vægt på andre aspekter. Dette er vigtigt, eftersom politikkerne på området med frihed, sikkerhed og retfærdighed ikke bør fremme en gradvis bevægelse hen imod et overvågningssamfund. EDPS forventer, at Rådet anlægger den samme tilgang i Stockholmprogrammet, også ved at anerkende retningslinjerne i punkt 25 nedenfor.

24. Dette er så meget desto mere vigtigt, som området med frihed, sikkerhed og retfærdighed er et område, der »præger borgernes levevilkår, navnlig det private rum for så vidt angår deres eget ansvar og personlige og sociale sikkerhed, der er beskyttet af de grundlæggende rettigheder«, hvilket for nylig blev fremhævet af den tyske forfatningsret i dom af 30. juni 2009 vedrørende Lissabontraktaten ([13]).

([9]) PNR-aftalen fra 2007 i den foregående fodnote og de, der gik forud.

([10]) Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (EUT L 105 af 13.4.2006, s. 54). Selv om retsgrundlaget er EF-traktatens artikel 95, var det en umiddelbar reaktion på bombeattentaterne i London.

([11]) Rådets rammeafgørelse 2008/977/RIA af 27. november 2008 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager (EUT L 350 af 30.12.2008, s. 60).

([12]) Jf. meddelelsens titel.

([13]) Pressemeddelelse nr. 72/2009 af 30. juni 2009 fra den tyske forfatningsdomstol, punkt 2, li-tra c).

25. EDPS understreger følgende i forbindelse med et sådant område:

— Der bør udveksles oplysninger mellem medlemsstaternes myndigheder, herunder hvor det er relevant, europæiske organer eller databaser, på grundlag af passende og effektive mekanismer, som fuldt ud respekterer borgernes grundlæggende rettigheder og sikrer gensidig tillid.

— Dette kræver ikke kun oplysningernes tilgængelighed kombineret med gensidig anerkendelse af medlemsstaternes (og EU's) retssystemer, men også en harmonisering af reglerne for beskyttelse af oplysninger, for eksempel, men ikke udelukkende, via en fælles databeskyttelsesramme.

— Disse fælles regler bør ikke kun gælde for situationer med grænseoverskridende dimensioner. Der kan kun eksistere gensidig tillid, når reglerne er solide og altid overholdes, uden risiko for at de ikke gælder, når den grænseoverskridende dimension ikke eller ikke længere er indlysende. Desuden kan forskelle mellem »interne« og »grænseoverskridende« data ikke fungere i praksis, især når det drejer sig om anvendelse af oplysninger ([14]).

V. **INSTRUMENTER MED HENBLIK PÅ DATABESKYTTELSE**

V.1. **Henimod en omfattende databeskyttelsesordning**

26. EDPS tilslutter sig den strategiske tilgang med hensyn til at give databeskyttelse en fremtrædende plads i meddelelsen. Mange initiativer inden for området med frihed, sikkerhed og retfærdighed hviler på anvendelsen af personoplysninger, og god databeskyttelse er afgørende for deres vellykkede gennemførelse. Respekt for privatlivets fred og databeskyttelse er ikke kun en retlig forpligtelse, der i stigende grad anerkendes på EU-plan, men det er også et spørgsmål, der er af afgørende betydning for de europæiske borgere, som det fremgår af resultaterne fra Eurobarometer ([15]). Endvidere er det også afgørende at begrænse adgangen til personoplysninger for at sikre de retshåndhævende myndigheders tillid.

27. I punkt 2.3 i meddelelsen hedder det, at der bør indføres en omfattende databeskyttelsesordning på samtlige EU's kompetenceområder ([16]). EDPS støtter fuldt ud dette mål uafhængigt af Lissabontraktatens ikrafttræden. Han noterer sig også, at en sådan ordning ikke nødvendigvis indebærer én retlig ramme, der gælder for al databehandling. I henhold til de nuværende traktater er mulighederne for at vedtage én omfattende retlig ramme, der gælder for al databehandling, begrænset på grund af søjlestrukturen og på grund af, at — i det mindste under første søjle — beskyttelse af oplysninger, der behandles af europæiske institutioner, finder sted på et særskilt retsgrundlag (EF-traktatens artikel 286). EDPS påpeger imidlertid, at der kan gennemføres nogle forbedringer ved fuldt ud at udnytte de muligheder, som de nuværende traktater indeholder, og som allerede er fremhævet af Kommissionen i meddelelsen om »Gennemførelsen af Haag-programmet: vejen frem« ([17]). Efter Lissabontraktatens ikrafttræden vil EU-traktatens artikel 16 indeholde det nødvendige retsgrundlag for én omfattende retlig ramme, der gælder for al databehandling.

28. EDPS noterer sig, at det — under alle omstændigheder — er afgørende at sikre konsekvens inden for den retlige ramme for databeskyttelse, hvor det er nødvendigt gennem harmonisering og konsolidering af de forskellige retsakter, der finder anvendelse på området med frihed, sikkerhed og retfærdighed.

I henhold til de nuværende traktater

29. Der blev for nylig taget et første skridt gennem vedtagelsen af Rådets rammeafgørelse 2008/977/RIA ([18]). Denne retsakt kan imidlertid ikke betragtes som en omfattende ramme, dybest set fordi dens bestemmelser ikke er almengyldige. De gælder ikke for interne situationer, hvor personoplysninger stammer fra den medlemsstat, der anvender dem. En sådan begrænsning vil nødvendigvis mindske den merværdi, der er forbundet med Rådets rammeafgørelse, medmindre samtlige medlemsstater beslutter at medtage interne situationer i den nationale gennemførelseslovgivning, hvilket ikke er sandsynligt.

30. En anden grund til, at EDPS finder, at Rådets rammeafgørelse 2008/977/RIA i det lange løb ikke indeholder en tilfredsstillende databeskyttelsesramme for så vidt angår området med frihed, sikkerhed og retfærdighed, er, at flere væsentlige bestemmelser ikke er i overensstemmelse med direktiv 95/46/EF. I henhold til de nuværende traktater kan der tages et yderligere skridt ved at udvide anvendelsesområdet og tilpasse Rådets rammeafgørelse til direktiv 95/46/EF.

31. Der kunne sættes yderligere skub i virkeliggørelsen af en omfattende databeskyttelsesordning ved at skabe en klar vision på lang sigt. Denne vision kunne indeholde en global og sammenhængende tilgang til definering af indsamling og udveksling af oplysninger — samt anvendelse af eksisterende databaser — sammen med

([14]) EDPS har uddybet det sidste punkt i sin udtalelse af 19. december 2005 om forslaget til Rådets rammeafgørelse om beskyttelse af personoplysninger i forbindelse med det politimæssige og strafferetlige samarbejde (KOM(2005) 475 endelig, EUT C 47 af 25.2.2006, s. 27, punkt 30-32).

([15]) Data Protection in the European Union — Citizens' perceptions — Analytical report, Flash Eurobarometer Series 225, Jan. 2008, http://www.ec.europa.eu/public_opinion/flash/fl_225_en.pdf

([16]) Jf. også de prioriterede retningslinjer i meddelelsen.

([17]) KOM(2006) 331 endelig af 28. juni 2006.

([18]) Se fodnote 11.

databeskyttelsesgarantier. Visionen bør forhindre overflødig overlapning af instrumenter (og dermed af behandlingen af personoplysninger). Den bør også fremme EU-politikkernes sammenhæng på dette område samt tilliden til, hvordan de offentlige myndigheder håndterer oplysninger om borgerne. EDPS anbefaler, at Rådet fremhæver behovet for en klar vision på lang sigt i Stockholmprogrammet.

32. EDPS anbefaler ligeledes, at de foranstaltninger, der allerede er vedtaget på dette område, og deres konkrete gennemførelse og effektivitet skal evalueres og ses i det rette perspektiv. Denne evaluering bør tage behørigt hensyn til omkostningerne for privatlivets fred og effektiviteten af retshåndhævelsen. Hvis disse evalueringer skulle vise, at visse foranstaltninger ikke giver de forventede resultater eller ikke står i rimeligt forhold til de mål, der forfølges, bør følgende skridt tages op til overvejelse:

— Som første skridt ændre eller ophæve foranstaltningerne, i det omfang de ikke synes i tilstrækkelig grad at frembringe en konkret merværdi for retshåndhævelsesmyndighederne og for de europæiske borgere

— Som andet skridt vurdere mulighederne for at forbedre anvendelsen af de eksisterende foranstaltninger

— Først som tredje skridt foreslå nye lovgivningsmæssige foranstaltninger, hvis det er sandsynligt, at disse nye foranstaltninger er nødvendige med henblik på de påtænkte mål. Der bør kun vedtages nye instrumenter, hvis de har en klar og konkret merværdi for retshåndhævelsesmyndighederne og for de europæiske borgere.

EDPS anbefaler, at der i Stockholmprogrammet henvises til et system for evaluering af eksisterende foranstaltninger.

33. Sidst men ikke mindst bør der lægges særlig vægt på en bedre gennemførelse af eksisterende garantier i overensstemmelse med Kommissionens meddelelse om opfølgning på arbejdsprogrammet for en bedre gennemførelse af databeskyttelsesdirektivet ([19]) og de forslag, som EDPS fremsatte i sin udtalelse om den pågældende meddelelse ([20]). Desværre har Kommissionen under tredje søjle ikke mulighed for at indlede overtrædelsesprocedurer.

I henhold til Lissabontraktaten

34. Lissabontraktaten åbner mulighed for en egentlig omfattende databeskyttelsesramme. I henhold til artikel 16, stk. 2, i traktaten om Den Europæiske Unions funktionsmåde skal Rådet og Europa-Parlamentet fastsætte regler for databeskyttelse i forbindelse med behandling af personoplysninger foretaget af Unionens institutioner, organer, kontorer og agenturer samt af medlemsstaterne under udøvelse af aktiviteter, der er omfattet af EU-retten, og af private parter.

35. EDPS forstår den vægt, der i meddelelsen lægges på en omfattende databeskyttelsesordning som Kommissionens ambition i forbindelse med at foreslå en retlig ramme, der gælder for alle behandlingsaktiviteter. Han tilslutter sig fuldt ud denne ambition, der styrker systemets sammenhæng, sikrer retssikkerheden og herved forbedrer beskyttelsen. Dette ville især i fremtiden forhindre vanskelighederne med at finde frem til en skillelinje mellem søjlerne, når oplysninger, der er indsamlet i den private sektor i kommercielt øjemed, senere hen anvendes til retshåndhævelsesformål. Denne skillelinje mellem søjlerne afspejler ikke fuldstændigt virkeligheden, hvilket fremgår af de vigtige domme, som Domstolen har afsagt i forbindelse med PNR ([21]) og lagring af data ([22]).

36. EDPS foreslår at fremhæve denne begrundelse for en omfattende databeskyttelsesordning i Stockholmprogrammet. Dette viser, at en sådan ordning ikke blot drejer sig om en præference, men om en nødvendighed, der finder sin begrundelse i den skiftende praksis for så vidt angår anvendelse af oplysninger. Han anbefaler, at det i Stockholmprogrammet som en prioritet anføres, at der er behov for en ny retlig ramme, blandt andet ved at erstatte Rådets rammeafgørelse 2008/977/RIA.

37. EDPS understreger, at begrebet omfattende databeskyttelsesordning baseret på en generel retlig ramme, ikke udelukker vedtagelsen af supplerende regler for databeskyttelse for politiet og retsvæsenet. Disse supplerende regler vil kunne tage hensyn til retshåndhævelsens specifikke behov, som omhandlet i erklæring 21, der er knyttet som bilag til Lissabontraktaten ([23]).

V.2. **Gentagelse af databeskyttelsesprincipperne**

38. I meddelelsen noteres det, at den teknologiske udvikling medfører forandringer i kommunikationen mellem individer og offentlige og private organisationer. På den baggrund er det ifølge Kommissionen nødvendigt at gentage en række grundlæggende databeskyttelsesprincipper.

([19]) KOM(2007) 87 endelig af 7. marts 2007.

([20]) Udtalelse af 25. juli 2007 (EUT C 255 af 27.10.2007, s. 1, særlig punkt 30).

([21]) Domstolens dom af 30. maj 2006, Europa-Parlamentet mod Rådet for Den Europæiske Union (C-317/04) og Kommissionen for De Europæiske Fællesskaber (C-318/04), forenede sager C-317/04 og C-318/04, Sml. 2006, s. I-4721.

([22]) Domstolens dom af 10. februar 2009, Irland mod Europa-Parlamentet og Rådet for Den Europæiske Union, sag C-301/06, endnu ikke offentliggjort.

([23]) Jf. erklæring 21 om beskyttelse af personoplysninger inden for retligt samarbejde i straffesager og politisamarbejde, der er knyttet som bilag til slutakten fra den regeringskonference, der vedtog Lissabontraktaten (EUT C 115 af 9.5.2008, s. 345).

39. EDPS ser med tilfredshed på disse hensigter i meddelelsen. En evaluering af effektiviteten af disse principper på baggrund af de teknologiske forandringer er særdeles nyttig. Det er først og fremmest vigtigt at notere, at en gentagelse og bekræftelse af databeskyttelsesprincipper ikke altid skal hænge direkte sammen med den teknologiske udvikling. Der vil også kunne være behov herfor i lyset af andre perspektiver, nævnt i del III ovenfor, nemlig internationalisering, stigende anvendelse af data til retshåndhævelse og fri bevægelighed.

40. Endvidere er EDPS af den opfattelse, at denne evaluering kan medtages i den offentlige høring, som Kommissionen bebudede på konferencen »Personal data — more use, more protection?«, der fandt sted den 19.-20. maj 2009. Denne offentlige høring vil kunne udgøre et værdifuldt bidrag ([24]). EDPS foreslår, at Rådet i teksten til Stockholmprogrammet og Kommissionen i sine offentlige erklæringer vedrørende høringen fremhæver forbindelsen mellem de hensigter, der er omhandlet i punkt 2.3 i meddelelsen, og den offentlige høring vedrørende fremtiden for databeskyttelse.

41. Til illustration af hvad en sådan evaluering vil kunne omfatte, anføres følgende punkter:

— Personoplysninger inden for området med frihed, sikkerhed og retfærdighed vil sandsynligvis være af en særlig følsom art, såsom oplysninger vedrørende straffedomme, politioplysninger og biometriske data som f.eks. fingeraftryk og dna-profiler.

— Behandlingen af disse oplysninger kan have negative følger for de registrerede, navnlig under hensyntagen til retshåndhævende myndigheders tvangsbeføjelser. Endvidere bliver dataovervågning og -analyse mere og mere automatiseret og foregår ofte uden menneskelige indgreb. Teknologi giver mulighed for at anvende databaser med personoplysninger med henblik på generelle søgninger (data mining, profilanalyse, osv.). De retlige forpligtelser, som databehandlingen er baseret på, bør fastlægges præcist.

— Det er en hjørnesten i databeskyttelseslovgivningen, at personoplysninger skal indsamles til bestemte formål og ikke må anvendes på en måde, der er uforenelig med disse formål. Anvendelse til formål, der er uforenelige, bør kun være tilladt, hvis det er fastsat ved lov og nødvendigt for at forfølge specifikke samfundsinteresser, som fastsat i artikel 8, stk. 2, i den europæiske menneskerettighedskonvention.

— Behovet for at respektere princippet om formålsbegrænsning kunne have konsekvenser for de aktuelle tendenser inden for dataanvendelse. I forbindelse med retshåndhævelse anvendes der oplysninger, der indsamles af private virksomheder i kommercielt øjemed i telekommunikations-, transport- og finanssektorerne. Endvidere oprettes der storstilede informationssystemer, for eksempel inden for områder som indvandring og grænsekontrol. Desuden er sammenkoblinger og adgang til databaser tilladt, hvorved de formål, som personoplysningerne oprindeligt blev indsamlet til, udvides. Der er behov for overvejelser vedrørende disse aktuelle tendenser, herunder eventuelle tilpasninger og/eller supplerende garantier, hvor det er nødvendigt.

— Ud over de principper for beskyttelse af oplysninger, der er omhandlet i meddelelsen, bør man i evalueringen være opmærksom på behovet for gennemsigtighed i forbindelse med databehandlingen og give den registrerede mulighed for at udøve sine rettigheder. Gennemsigtighed er et særligt vanskeligt spørgsmål på retshåndhævelsesområdet, især fordi gennemsigtighed bør afvejes mod de risici, som efterforskningerne vil kunne udsættes for.

— Der bør findes frem til løsninger vedrørende udvekslinger med tredjelande.

42. Denne evaluering bør endvidere fokusere på mulighederne for at forbedre effektiviteten af databeskyttelsesprincippernes anvendelse. I den forbindelse kunne det være nyttigt at koncentrere sig om de instrumenter, der kan styrke de registeransvarliges ansvar. Disse instrumenter skal give mulighed for fuld ansvarliggørelse af de registeransvarlige for så vidt angår datahåndtering. »Data governance« er et nyttigt begreb i denne forbindelse. Dette omfatter alle retlige, tekniske og organisatoriske midler, som organisationer anvender for at sikre fuldt ansvar for den måde, som oplysningerne håndteres på, såsom planlægning og kontrol, anvendelse af forsvarlig teknologi, passende uddannelse af personale, kontrol af overensstemmelse, osv.

V.3. **Teknologi, der tilgodeser hensynet til privatlivet**

43. EDPS glæder sig over, at punkt 2.3 i meddelelsen omhandler certificering af teknologi, der er »privatlivsvenlig«. Derudover kunne der henvises til »indbygget databeskyttelse« (»privacy by design«) og behovet for at indkredse »bedste tilgængelige teknikker«, der er i overensstemmelse med EU's databeskyttelsesramme.

44. EDPS mener, at »indbygget databeskyttelse« og teknologier, der tilgodeser hensynet til privatlivet, kunne være nyttige redskaber til en bedre beskyttelse samt en mere effektiv anvendelse af oplysninger. EDPS foreslår to veje fremad — der ikke udelukker hinanden:

— En ordning for certificering i forbindelse med privatlivets fred og databeskyttelse ([25]) som en valgmulighed for udviklere og brugere af informationssystemer, hvad enten de får støtte via EU-midler eller EU-lovgivning eller ikke.

([24]) Artikel 29-Gruppen vedrørende Beskyttelse af Personoplysninger, som EDPS deltager i, har besluttet at arbejde intensivt med sit bidrag til denne offentlige høring.

([25]) Et eksempel på en sådan ordning er den europæiske datasikkerhedsmærkning (EuroPriSe).

— En retlig forpligtelse for udviklere og brugere af informationssystemer til at anvende systemer, der er i overensstemmelse med princippet om indbygget databeskyttelse. Dette vil kunne gøre det nødvendigt at udvide databeskyttelseslovgivningens nuværende anvendelsesområde, således at systemudviklere gøres ansvarlige for de informationssystemer, de udvikler ([26]).

EDPS foreslår, at disse mulige veje fremad nævnes i Stockholmprogrammet.

V.4. **Eksterne aspekter**

45. Et andet emne, der er nævnt i meddelelsen, er udviklingen af og arbejdet hen mod interna-tionale standarder for databeskyttelse. For øjeblikket finder der mange aktiviteter sted med henblik på at indføre gennemførlige standarder for global anvendelse, for eksempel i forbindelse med den internationale konference for databeskyttelsesmyndigheder og -ansvarlige. I den nærmeste fremtid kunne dette føre til en international aftale. EDPS foreslår, at Stockholmprogrammet støtter disse aktiviteter.

46. I meddelelsen omhandles også indgåelse af bilaterale aftaler, der er baseret på de fremskridt, der er allerede er gjort sammen med USA. EDPS er enig i, at der er behov for en klar retlig ramme for videregivelse af data til tredjelande, og hilser derfor det fælles arbejde velkommen, som EU's og USA's myndigheder har udført i Kontaktgruppen på Højt Plan om et eventuelt transatlantisk databeskyttelsesinstrument, men ønsker samtidig mere klarhed og opmærksomhed om bestemte spørgsmål ([27]). På den baggrund er det også interessant at notere sig idéerne i rapporten om indre anliggender til et Euro-atlantisk samarbejdsområde vedrørende frihed, sikkerhed og retfærdighed, som EU i henhold til rapporten skal tage stilling til senest i 2014. Et sådant område vil ikke være muligt uden passende databeskyttelsesgarantier.

47. Ifølge EDPS bør de europæiske standarder for databeskyttelse, der er baseret på Europarådets konvention nr. 108 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger ([28]), og Domstolens og Menneskerettighedsdomstolens retspraksis, bestemme beskyttelsesniveauet i en generel aftale med USA om databeskyttelse og dataudveksling. En sådan generel aftale kunne danne grundlaget for særlige ordninger for udveksling af personoplysninger. Dette er endnu vigtigere i lyset af, at det i henhold til punkt 4.2.1 i meddelelsen er hensigten, at Den Europæiske Union, hvor det er nødvendigt, bør indgå aftaler om politisamarbejde.

48. EDPS forstår fuldt ud, at der er behov for at styrke det internationale samarbejde, i nogle tilfælde også med lande, der ikke beskytter de grundlæggende rettigheder. Det er imidlertid ([29]) af afgørende betydning, at der tages hensyn til, at dette internationale samarbejde sandsynligvis vil medføre en stor stigning i indsamling og international videregivelse af oplysninger. Det er derfor afgørende, at principperne om retfærdig og lovlig behandling — såvel som principperne om behørig behandling i almindelighed — kommer til at gælde for indsamling og videregivelse af personoplysninger på tværs af EU's ydre grænser, og at personoplysninger kun overføres til tredjelande eller internationale organer eller organisationer, hvis de berørte tredjeparter garanterer et passende beskyttelsesniveau eller giver andre passende garantier.

49. Afslutningsvis anbefaler EDPS, at man i Stockholmprogrammet fremhæver betydningen af generelle aftaler med USA og andre tredjelande om databeskyttelse og dataudveksling på grundlag af det beskyttelsesniveau, der er garanteret inden for EU's område. Set ud fra et bredere perspektiv peger EDPS på betydningen af, at respekten for de grundlæggende rettigheder aktivt fremmes, og især for databeskyttelse, i forbindelse med tredjelande og med internationale organisationer ([30]). Endvidere kunne man i Stockholmprogrammet omtale det generelle begreb om, at udveksling af personoplysninger med tredjelande fordrer et tilstrækkeligt beskyttelsesniveau eller andre passende garantier i de pågældende tredjelande.

VI. **BRUG AF OPLYSNINGER**

VI.1. **Hen imod en europæisk informationsmodel**

50. Bedre udveksling af oplysninger er et væsentligt mål for Den Europæiske Union på området med frihed, sikkerhed og retfærdighed. I punkt 4.1.2 i meddelelsen understreges det, at sikkerheden i Den Europæiske Union hviler på stærke mekanismer for informationsudveksling mellem de nationale myndigheder og de europæiske aktører. Denne betoning af informationsudveksling er logisk i betragtning af, at der ikke findes en europæisk politistyrke, et europæisk

([26]) Informationsbrugere er omfattet af databeskyttelseslovgivningen, ligesom registeransvarlige eller databehandlere.

([27]) Jf. EDPS's udtalelse af 11. november 2008 om den endelige rapport fra EU-USA-Kontaktgruppen på Højt Plan om Informationsdeling og Beskyttelse af Privatlivets Fred og Personoplysninger (EUT C 128 af 6.6.2009, s. 1).

([28]) ETS nr. 108 af 28.1.1981.

([29]) Jf. EDPS's skrivelse af 28. november 2005 om Kommissionens meddelelse om den eksterne dimension af området med frihed, sikkerhed og retfærdighed, der er tilgængelig på den tilsynsførendes websted.

([30]) Seneste retspraksis vedrørende lister over terrorister bekræfter, at der er behov for garantier — også i forbindelserne med De Forenede Nationer — for at sikre, at foranstaltningerne til bekæmpelse af terrorisme overholder EU's standarder vedrørende grundlæggende rettigheder (forenede sager C-402/05 P og C-415/05 P, Kadi og Al Barakaat International Foundation mod Rådet , dom af 3. september 2008, endnu ikke offentliggjort).

strafferetligt system og en europæisk grænsekontrol. Foranstaltninger vedrørende oplysninger er derfor væsentlige bidrag fra Den Europæiske Union, der giver medlemsstaternes myndigheder mulighed for at tackle grænseoverskridende kriminalitet på en effektiv måde og for effektivt at beskytte de ydre grænser. De bidrager imidlertid ikke kun til borgernes sikkerhed men også til deres frihed — fri bevægelighed for personer blev nævnt tidligere som et perspektiv i denne udtalelse — og til retfærdighed.

51. Det er netop af disse grunde, at tilgængelighedsprincippet blev indført i Haagprogrammet. Det indebærer, at oplysninger, der er nødvendige for at bekæmpe kriminalitet, uden hindringer bør kunne passere de indre grænser i EU. Nye erfaringer viser, at det var vanskeligt at gennemføre dette princip i lovgivningsforanstaltninger. Kommissionens forslag til Rådets rammeafgørelse om udveksling af oplysninger efter tilgængelighedsprincippet af 12. oktober 2005 ([31]) blev ikke accepteret i Rådet. Medlemsstaterne var ikke rede til fuldt ud at acceptere konsekvenserne af tilgængelighedsprincippet. Der blev i stedet vedtaget mere begrænsede instrumenter ([32]) såsom Rådets afgørelse 2008/615/RIA af 23. juni 2008 om intensivering af det grænseoverskridende samarbejde, navnlig om bekæmpelse af terrorisme og grænseoverskridende kriminalitet (»Prümaftalen«) ([33]).

52. Tilgængelighedsprincippet var et centralt aspekt af Haagprogrammet, men Kommissionen synes nu at have en mere beskeden tilgang. Den påtænker at stimulere udvekslingen af oplysninger mellem medlemsstaternes myndigheder yderligere ved at indføre den europæiske informationsmodel. Det svenske EU-formandskabs går i samme retning ([34]). Den vil forelægge et forslag til en strategi for informationsudveksling. Rådet har allerede indledt arbejdet med dette ambitiøse projekt vedrørende en EU-informationsstyringsstrategi, der er tæt knyttet til den europæiske informationsmodel. EDPS noterer sig denne udvikling med stor interesse og fremhæver den vægt, der bør lægges på databeskyttelseselementerne i disse projekter.

En europæisk informationsmodel og databeskyttelse

53. Det skal som udgangspunkt fremhæves, at fremtiden for området med frihed, sikkerhed og retfærdighed ikke bør være »teknologidrevet« i den forstand, at de næsten ubegrænsede muligheder, som de nye teknologier tilbyder, altid bør kontrolleres på baggrund af de relevante databeskyttelsesprincipper og kun anvendes, hvis de overholder disse principper.

54. EDPS noterer sig, at informationsmodellen præsenteres i meddelelsen ikke kun som en teknisk model: en styrket strategisk analysekapacitet og en bedre indsamling og behandling af operationelle oplysninger. Det anerkendes også, at politikrelaterede aspekter — såsom kriterier for indsamling, videregivelse og behandling af oplysninger — bør tages i betragtning, samtidig med at databeskyttelsesprincipperne overholdes.

55. Informationsteknologi og retlige betingelser er — og vil fortsat være — af afgørende betydning. EDPS ser med tilfredshed på meddelelsen, der tager udgangspunkt i den antagelse, at tekniske betragtninger ikke kan ligge til grund for en europæisk informationsmodel. Det er afgørende, at oplysningerne udelukkende indsamles, videregives og behandles på grundlag af konkrete behov for sikkerhed og under hensyntagen til databeskyttelsesprincipperne. EDPS tilslutter sig også helt behovet for at fastlægge en opfølgningsmekanisme for vurdering af, hvordan informationsudvekslingen fungerer. Han foreslår, at Rådet uddyber disse elementer i Stockholmprogrammet.

56. I den forbindelse understreger EDPS, at databeskyttelse, der tager sigte på at beskytte borgerne, ikke bør ses som en hæmsko for effektiv datahåndtering. Den tilvejebringer vigtige redskaber til forbedring af lagring af, adgang til og udveksling af oplysninger. Den registreredes ret til at blive orienteret om, hvilke oplysninger vedrørende den registrerede selv der behandles, og til at foretage berigtigelse af ukorrekte oplysninger kan også styrke rigtigheden af oplysninger i datahåndteringssystemerne.

57. Databeskyttelseslovgivningen har i det væsentlige følgende konsekvenser: hvis der er brug for data til et specifikt og legitimt formål, kan de anvendes; hvis der ikke er brug for dem til et veldefineret formål, bør personoplysninger ikke anvendes. I det første tilfælde kan der være brug for supplerende foranstaltninger til at sørge for passende garantier.

58. EDPS forholder sig imidlertid kritisk til meddelelsens omtale af »kortlægning af fremtidige behov« som en del af informationsmodellen. Han fremhæver, at også i fremtiden bør princippet om formålsbegrænsning være en rettesnor, når der udvikles informationssystemer ([35]). En af de væsentligste garantier, som databeskyttelsessystemet yder borgerne, er følgende: den pågældende skal på forhånd være bekendt med, til hvilket formål oplysninger vedrørende den pågældende indsamles, og at de udelukkende vil blive brugt til det formål, også i fremtiden. Denne garanti er endog nedfældet i artikel 8 i EU's charter om grundlæggende rettigheder. Princippet om formålsbegrænsning giver mulighed for undtagelser hvilket især er relevant på området med frihed, sikkerhed og retfærdighed men disse undtagelser bør ikke bestemme udviklingen af et system.

([31]) KOM(2005) 490 endelig udg.
([32]) For så vidt angår tilgængelighed; Prümaftalen indeholder vidtrækkende bestemmelser for anvendelsen af biometriske oplysninger (dna og fingeraftryk).
([33]) EUT L 210 af 6.8.2008, s. 1.
([34]) Jf. regeringernes EU-arbejdsprogram, der er nævnt i fodnote 5, s. 23.
([35]) Jf. ligeledes punkt 41 ovenfor.

Valg af den rette arkitektur

59. Valg af den rette arkitektur for udveksling af oplysninger er udgangspunktet for det hele. I meddelelsen (punkt 4.1.3) anerkendes betydningen af en egentlig informationsarkitektur, men desværre kun i forbindelse med samkøring.

60. EDPS understreger et andet aspekt: inden for den europæiske informationsmodel bør databeskyttelseskravene være en integreret del af al systemudvikling og bør ikke blot betragtes som en nødvendig betingelse for et systems lovlighed ([36]). Man bør anvende begreberne »indbygget databeskyttelse«, og der er behov for at indkredse »bedste tilgængelige teknikker« ([37]) som omhandlet i punkt 43 ovenfor. Den europæiske informationsmodel bør være baseret på disse begreber. Dette betyder mere konkret, at informationssystemer, der er udformet med henblik på den offentlige sikkerhed, altid bør være udviklet i overensstemmelse med principperne for »indbygget databeskyttelse«. EDPS anbefaler, at Rådet medtager disse elementer i Stockholmprogrammet.

Samkøring af systemer

61. EDPS understreger, at samkøring ikke er et rent teknisk spørgsmål, men at det også har konsekvenser for beskyttelse af borgerne, navnlig databeskyttelse. Set fra et databeskyttelsesperspektiv indebærer samkøring af systemer, hvis det udføres godt, klare fordele med hensyn til at undgå dobbelt lagring. Det er imidlertid også indlysende, at det, at adgang til eller udveksling af data gøres teknisk muligt, i mange tilfælde bliver et kraftigt incitament til rent faktisk at konsultere eller udveksle disse data. Med andre ord indebærer samkøring særlige risici ved sammenkobling mellem databaser med forskellige formål ([38]). Det kan påvirke databasernes strenge formålsbegrænsninger.

62. Kort sagt er den kendsgerning, at det er teknisk muligt at udveksle digital information mellem databaser, der kan samkøres, eller at flette disse databaser ikke en begrundelse for en undtagelse fra princippet om formålsbegrænsning. Samkøring bør i konkrete tilfælde være baseret på klare og omhyggelige politiske valg. EDPS foreslår, at dette begreb præciseres i Stockholmprogrammet.

VI.2. **Anvendelse af oplysninger, der er indsamlet til andre formål**

63. Meddelelsen omhandler ikke udtrykkeligt en af de vigtigste tendenser i de seneste år, nemlig anvendelse af data, der er indsamlet i den private sektor i kommercielt øjemed, til retshåndhævelsesformål. Denne tendens vedrører ikke kun trafikdata i forbindelse med elektronisk kommunikation og passageroplysninger for personer, der flyver til (visse) tredjelande ([39]), men fokuserer også på den finansielle sektor. Et eksempel er Europa-Parlamentets og Rådets direktiv 2005/60/EF af 26. oktober 2005 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvaskning af penge og finansiering af terrorisme ([40]). Et andet velkendt og meget omtalt eksempel vedrører behandling af personoplysninger i Society for Worldwide Interbank Financial Telecommunication (SWIFT) ([41]) for så vidt angår data, der er nødvendige for det amerikanske finansministeriums program til sporing af finansiering af terrorisme.

64. EDPS mener, at disse tendenser kræver særlig opmærksomhed i Stockholmprogrammet. De kan betragtes som undtagelser fra princippet om formålsbegrænsning og griber ofte meget ind i privatlivets fred, eftersom anvendelsen af disse data kan afsløre meget om enkeltpersoners adfærd. I hvert tilfælde, hvor der foreslås sådanne foranstaltninger, skal der være meget stærke beviser for, at en sådan indgribende foranstaltning er nødvendig. Hvis der forelægges sådanne beviser, skal det sikres, at personernes rettigheder beskyttes fuldt ud.

65. Ifølge EDPS bør der kun være mulighed for at anvende personoplysninger, der er indsamlet i kommercielt øjemed, til retshåndhævelsesformål på strenge betingelser, som f.eks.:

— Data anvendes kun til specifikt definerede formål, som f.eks. bekæmpelse af terrorisme eller alvorlig kriminalitet, der skal fastlægges fra gang til gang.

— Data videregives via et »push«-system og ikke et »pull«-system ([42]).

([36]) Jf. »Guidelines and criteria for the development, implementation and use of Privacy Enhancing Security Technologies« udarbejdet i forbindelse med PRISE-projektet (http://www.prise.oeaw.ac.at).

([37]) Med den bedste tilgængelige teknik menes der det mest effektive og avancerede trin i udviklingen af aktiviteter og driftsmetoder, som er udtryk for en given tekniks principielle praktiske egnethed som grundlag for, at ITS-applikationer og -systemer overholder kravene vedrørende privatlivets fred, databeskyttelse og sikkerhed, der er fastlagt i EU's lovramme.

([38]) Jf. den tilsynsførendes bemærkninger til Kommissionens meddelelse om kompatibilitet mellem europæiske databaser, 10.3.2006, der findes på: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

([39]) Jf. f.eks. punkt 15 ovenfor.

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

([41]) Jf. udtalelse 10/2006 om behandling af personoplysninger i Society for Worldwide Interbank Financial Telecommunication (SWIFT) fra Artikel 29-Gruppen.

([42]) I forbindelse med »push«-systemet sender den registeransvarlige dataene efter anmodning (»pushes«) til den retshåndhævende myndighed. I forbindelse med »pull«-systemet har den retshåndhævende myndighed adgang til den ansvarliges database og udtrækker (»pulls«) oplysningerne fra den database. I forbindelse med »pull«-systemet er det mere vanskeligt for den registeransvarlige at varetage sit ansvar.

— Anmodninger om data bør stå i rimeligt forhold til formålet, være meget målrettede og i princippet være baseret på mistanker, der rettet mod bestemte personer.

— Rutinesøgninger, data mining og profilanalyse bør undgås.

— Al anvendelse af data til retshåndhævelsesformål bør logges for at give den registrerede, der udøver sine rettigheder, databeskyttelsesmyndighederne og retsvæsenet mulighed for effektivt at kontrollere anvendelsen.

VI.3. **Informationssystemer og EU-organer**

Informationssystemer med eller uden central lagring ([43])

66. I løbet af de seneste år er antallet af informationssystemer baseret på EU-lovgivning vokset i betydelig grad inden for området med frihed, sikkerhed og retfærdighed. Sommetider træffes der afgørelser for at indføre et system, der medfører central lagring af data på europæisk plan, til andre tider omhandler lovgivningen kun udveksling af oplysninger mellem nationale databaser. Schengeninformationssystemet er formodentligt det bedste eksempel på et system med central lagring. Rådets afgørelse 2008/615/RIA (Prümaftalen) ([44]) er set fra et databeskyttelsesperspektiv det væsentligste eksempel på et system uden central lagring, da det forudser en omfattende udveksling af biometriske data mellem medlemsstaternes myndigheder.

67. Meddelelsen belyser, at denne tendens med at indføre nye systemer vil fortsætte. Et første eksempel, der er taget fra punkt 4.2.2, er et informationssystem, der udvider det europæiske informationssystem vedrørende strafferegistre (ECRIS) til at omfatte tredjelandsstatsborgere. Kommissionen har allerede bestilt en undersøgelse vedrørende det europæiske register over dømte statsborgere fra tredjelande (European Index for Convicted Third Country Nationals — EICTCN), hvilket eventuelt vil føre til en central database. Et andet eksempel er udvekslingen af oplysninger om personer i forbindelse med insolvensregistre i andre medlemsstater inden for rammerne af e-justice (punkt 3.4.1 i meddelelsen) uden central lagring.

68. Et decentralt system vil have visse fordele set fra et databeskyttelsesperspektiv. Herved undgås det, at medlemsstatens myndighed og det centrale system foretager dobbelt lagring, ansvaret for dataene er klart, eftersom medlemsstatens myndighed er den registeransvarlige, og retsvæsenets og databeskyttelsesmyndighedernes kontrol kan finde sted på medlemsstatsplan. Men dette system har også svagheder, når data udveksles med andre jurisdiktioner, for eksempel når det skal sikres, at oplysninger ajourføres både i oprindelseslandet og i bestemmelseslandet, og med hensyn til at sikre effektiv kontrol på begge sider. Det er endnu vanskeligere at sikre ansvaret for det tekniske system for udvekslingen. Disse svagheder kan klares ved at vælge et centralt system, hvor de europæiske organer har et ansvar i det mindste for dele af systemet (som f.eks. den tekniske infrastruktur).

69. I den forbindelse ville det være nyttigt at opstille vægtige kriterier for valget mellem centrale og decentrale systemer, idet der sikres klare og omhyggelige politiske valg i de konkrete tilfælde. Disse kriterier kan bidrage til systemernes funktion samt til beskyttelsen af borgernes data. EDPS foreslår at anføre, at det er hensigten at opstille sådanne kriterier i Stockholmprogrammet.

Storstilede informationssystemer

70. I punkt 4.2.3.2 i meddelelsen drøftes i korte træk fremtiden for storstilede informationssystemer med særlig vægt på Schengeninformationssystemet (SIS) og visuminformationssystemet (VIS).

71. Punkt 4.2.3.2 omhandler også indførelsen af et system for elektronisk registrering af indrejse til og udrejse fra EU-medlemsstaternes område samt programmer for registrerede rejsende. Kommissionen har allerede på et tidligere tidspunkt omtalt dette system som led i »grænsepakken« på foranledning af næstformand Franco Frattini ([45]). I sine indledende bemærkninger ([46]) var EDPS forholdsvis kritisk over for dette forslag, da behovet for et sådant indgribende system oven i de eksisterende storstilede systemer ikke var tilstrækkeligt påvist. EDPS har ikke noteret, at der er yderligere dokumentation for behovet for et sådant system, og foreslår derfor Rådet, at det ikke nævner denne idé i Stockholmprogrammet.

72. I den forbindelse ønsker EDPS at henvise til sine udtalelser om forskellige initiativer vedrørende EU's informationsudveksling ([47]), hvori han fremsatte en lang række forslag og bemærkninger om den indvirkning på databeskyttelse, som anvendelsen af store databaser på EU-plan har. Blandt andre spørgsmål lagde han særlig vægt på behovet for stærke og skræddersyede garantier, der bør være indført, samt konsekvensanalysers proportionalitet og nødvendighed, inden der foreslås eller iværksættes foranstaltninger

([43]) Central lagring skal i denne sammenhæng forstås som lagring på et centralt europæisk plan, mens decentral lagring betyder lagring på medlemsstatsplan.

([44]) Se fodnote 33.

([45]) Meddelelse fra Kommissionen — Forberedelse af de kommende faser af grænseforvaltningen i EU (KOM(2008) 69 endelig af 13.2.2008).

([46]) Indledende bemærkninger fra EDPS om tre meddelelser fra Kommissionen om grænseforvaltning KOM(2008) 69, KOM(2008) 68 og KOM(2008) 67 af 3. marts 2008 der findes på: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf

([47]) Især skal nævnes følgende: Udtalelse af 23. marts 2005 om forslaget til Europa-Parlamentets og Rådets forordning om visuminformationssystemet (VIS) og udveksling af oplysninger mellem medlemsstaterne om visa til kortvarigt ophold (EUT C 181 af 23.7.2005, s. 13) og udtalelse af 19. oktober 2005 om tre forslag vedrørende anden generation af Schengen-informationssystemet (SIS II) (EUT C 91 af 19.4.2006, s. 38).

på dette område. EDPS er altid gået ind for en balance, der sikrer beskyttelse af rettigheder og data, mellem på den ene side sikkerhedskrav og på den anden side beskyttelse af de personers privatliv, som er omfattet af systemerne. Han indtog samme holdning, da han var tilsynsførende for de centrale del af systemerne.

73. Endvidere benytter EDPS denne lejlighed til at fremhæve behovet for en konsekvent tilgang til EU's informationsudveksling som helhed for så vidt angår konsekvens vedrørende retlige og tekniske aspekter samt tilsynsaspekter mellem de systemer, der allerede er indført, og dem, der er under udvikling. Nu til dags er der mere end nogensinde et klart behov for en modig og omfattende vision om, hvordan EU's informationsudveksling og fremtiden for storstilede informationssystemer bør se ud. Det vil kun være muligt at tage et elektronisk system for indrejse til og udrejse fra medlemsstaternes område op til overvejelse på grundlag af en sådan vision.

74. EDPS foreslår, at der i Stockholmprogrammet henvises til, at det er hensigten at udvikle en sådan vision, der også bør afspejle Lissabontraktatens eventuelle ikrafttræden og dens indvirkning på de systemer, der er baseret på retsgrundlag under første og tredje søjle.

75. Endelig omhandler meddelelsen oprettelsen af et nyt agentur, der ifølge meddelelsen også bør være kompetent med hensyn til det elektroniske system for indrejse og udrejse. I mellemtiden har Kommissionen vedtaget et forslag om oprettelsen af et sådant agentur ([48]). EDPS støtter i princippet dette forslag, da det kan medvirke til, at disse systemer, herunder databeskyttelse, fungerer mere effektivt. Han vil forelægge en udtalelse om dette forslag, når tiden er inde.

Europol og Eurojust

76. Europols rolle omtales flere steder i meddelelsen, hvilket understreger, at Europol skal spille en central rolle i forbindelse med koordinering, informationsudveksling og uddannelse af fagfolk, og at dette er et prioriteret område. Ligeledes henvises der i punkt 4.2.2 i meddelelsen til ændringerne for nylig af de retlige rammer for samarbejdet mellem Eurojust og Europol, og det oplyses, at Eurojust bør styrkes yderligere, navnlig for så vidt angår efterforskning af grænseoverskridende organiseret kriminalitet. EDPS støtter fuldt disse mål under forudsætning af, at databeskyttelsesgarantier respekteres på passende måde.

77. I den forbindelse ser EDPS med tilfredshed på det nye udkast til aftale, som man for nylig nåede frem til mellem Europol og Eurojust ([49]), og som tager sigte på at forbedre og styrke det gensidige samarbejde mellem de to organer og sørge for effektiv informationsudveksling mellem dem. Dette er et arbejde, hvor effektiv og velfungerende databeskyttelse spiller en afgørende rolle.

VI.4. **Anvendelse af biometriske data**

78. EDPS noterer, at meddelelsen ikke behandler spørgsmålet om den stigende anvendelse af biometriske data i Den Europæiske Unions forskellige retsakter vedrørende anvendelse af informationsudveksling, herunder instrumenter, der indfører storstilede informationssystemer. Dette er beklageligt i betragtning af, at det er et emne, der er meget vigtigt og følsomt set i lyset af databeskyttelse og beskyttelse af privatlivets fred.

79. Selv om EDPS erkender de generelle fordele ved at anvende biometriske data, har han til stadighed understreget de omfattende virkninger af at anvende disse data på personers rettigheder og foreslået, at der indarbejdes strenge beskyttelsesforanstaltninger i forbindelse med anvendelsen af biometriske data i hvert enkelt system. Den Europæiske Menneskerettighedsdomstols dom for nylig i sagen *S. og Marper mod Det Forenede Kongerige* ([50]) giver nyttige oplysninger i denne forbindelse, navnlig vedrørende begrundelsen og grænserne for anvendelsen af biometriske data. Især anvendelsen af dna-oplysninger kan afsløre følsomme oplysninger om enkeltpersoner, idet det også tages i betragtning, at de tekniske muligheder for at udtrække oplysninger fra dna stadig udvides. I tilfælde af storstilet anvendelse af biometriske data i informationssystemer er der også et problem på grund af, at der i sagens natur er unøjagtigheder i forbindelse med indsamling og sammenligning af biometriske data. Af disse grund bør EU-lovgiveren være tilbageholdende med at anvende disse data.

80. Et andet tilbagevendende spørgsmål i de seneste år har været anvendelsen af fingeraftryk fra børn og ældre på grund af de biometriske systemers iboende mangler for så vidt angår disse aldersgrupper. EDPS har anmodet om en tilbundsgående undersøgelse for at bestemme systemernes nøjagtighed ordentligt ([51]). Han har foreslået en aldersgrænse på 14 år for børn, medmindre andet fremgår af denne undersøgelse. EDPS anbefaler, at dette spørgsmål nævnes i Stockholmprogrammet.

([48]) Kommissionens forslag af 24. juni 2009 til Europa-Parlamentets og Rådets forordning om oprettelse af et agentur for den operationelle forvaltning af Schengeninformationssystemet (SIS II), visuminformationssystemet (VIS), Eurodac og andre store it-systemer inden for området frihed, sikkerhed og retfærdighed (KOM(2009) 293/2).

([49]) Udkast til aftale, godkendt af Rådet, men endnu ikke undertegnet af de to parter. Jf. Rådets register:
http://register.consilium.europa.eu/pdf/en/09/st10/st10019.en09.pdf
http://register.consilium.europa.eu/pdf/en/09/st10/st10107.en09.pdf

([50]) Forenede sager 30562/04 og 30566/04, S. og Marper mod Det Forenede Kongerige, dom af 4. december 2008, ECHR, endnu ikke offentliggjort.

([51]) Udtalelse af 26. marts 2008 om forslaget til en forordning om ændring af Rådets forordning (EF) nr. 2252/2004 om standarder for sikkerhedselementer og biometriske identifikatorer i pas og rejsedokumenter, som medlemsstaterne udsteder (EUT C 200 af 6.8.2008, s. 1).

81. Når dette er sagt, forslår EDPS, at det ville være nyttigt at opstille vægtige kriterier for anvendelsen af biometriske data. Disse kriterier bør sikre, at dataene kun anvendes, når det er nødvendigt, passende og står i rimeligt forhold til formålet, og når lovgiveren har godtgjort, at der er tale om udtrykkeligt angivne og legitime formål. For at være mere præcis bør biometriske data og især dna-oplysninger ikke anvendes, hvis den samme virkning kan opnås ved at anvende andre mindre følsomme oplysninger.

VII. **ADGANG TIL RETLIG PRØVELSE OG E-JUSTICE**

82. Teknologi vil også blive brugt som et redskab til bedre retligt samarbejde. I punkt 3.4.1 i meddelelsen anføres det, at e-justice gør det lettere for borgerne at indbringe sager for domstolene. Det består af en portal med information og videokonferencer som led i den juridiske procedure. Det giver endvidere mulighed for at iværksætte juridiske procedurer online, og i forbindelse hermed påtænkes det at sammenkoble nationale registre, som f.eks. insolvensregistre. EDPS noterer sig, at meddelelsen ikke omhandler nye initiativer vedrørende e-justice, men konsoliderer de tiltag, der allerede er iværksat. EDPS er involveret i nogle af disse tiltag som en opfølgning af den udtalelse, han afgav den 19. december 2008 om Kommissionens meddelelse »På vej mod en EU-strategi for e-justice« ([52]).

83. E-justice er et ambitiøst projekt, der kræver fuld støtte. Det kan på effektiv vis forbedre retsvæsenet i Europa og den retlige beskyttelse af borgerne. Det er et væsentligt skridt hen imod et europæisk område med retfærdighed. På baggrund af denne positive vurdering kan der fremsættes nogle bemærkninger:

— De teknologiske systemer i forbindelse med e-justice bør udvikles i overensstemmelse med princippet for »indbygget databeskyttelse«. Som tidligere nævnt i forbindelse med den europæiske informationsmodel er valget af den rette arkitektur udgangspunktet for det hele.

— Sammenkobling og samkøring mellem systemerne bør respektere princippet om formålsbegrænsning.

— De forskellige aktørers ansvarsområder bør nøje defineres.

— Konsekvenserne for enkeltpersoner af sammenkoblingen af nationale registre med følsomme personoplysninger, som f.eks. insolvensregistre, bør analyseres på forhånd.

VIII. **KONKLUSIONER**

84. EDPS tilslutter sig den vægt, der i meddelelsen lægges på beskyttelse af grundlæggende rettigheder, og navnlig beskyttelse af personoplysninger, som et af de centrale spørgsmål i forbindelse med fremtiden for området med frihed, sikkerhed og retfærdighed. Efter EDPS's opfattelse fremmer meddelelsen med rette en balance mellem behovene for passende instrumenter til at garantere borgerne sikkerhed og beskyttelsen af deres grundlæggende rettigheder. Det erkendes, at der bør lægges mere vægt på beskyttelsen af personoplysninger.

85. EDPS støtter fuldt ud punkt 2.3 i meddelelsen, hvori der opfordres til, at der indføres en omfattende databeskyttelsesordning på samtlige EU's kompetenceområder uafhængigt af Lissabontraktatens ikrafttræden. Han anbefaler i denne forbindelse:

— at det i Stockholmprogrammet anføres, at der er behov for en klar vision på lang sigt for en sådan omfattende ordning,

— at de foranstaltninger, der er vedtaget på dette område, og deres konkrete gennemførelse og effektivitet evalueres, idet der tages hensyn til omkostningerne for privatlivets fred og effektiviteten af retshåndhævelsen,

— at det i Stockholmprogrammet som en prioritet anføres, at der er behov for en ny retlig ramme, blandt andet ved at erstatte Rådets rammeafgørelse 2008/977/RIA.

86. EDPS udtrykker tilfredshed med, at Kommissionen har til hensigt at bekræfte databeskyttelsesprincipperne, der skal knyttes til den offentlige høring bebudet af Kommissionen på konferencen »Personal data — more use, more protection?«, der fandt sted den 19.-20. maj 2009. Med hensyn til substansen fremhæver EDPS betydningen af princippet om formålsbegrænsning som en hjørnesten i databeskyttelseslovgivningen og af at fokusere på mulighederne for at forbedre effektiviteten af databeskyttelsesprincippernes anvendelse ved hjælp af instrumenter, der kan styrke de registeransvarliges ansvar.

87. »Indbygget databeskyttelse« og teknologier, der tilgodeser hensynet til privatlivet, kunne fremmes ved

— en ordning for certificering i forbindelse med beskyttelse af privatlivets fred og databeskyttelse som en valgmulighed for udviklere og brugere af informationssystemer,

— en retlig forpligtelse for udviklere og brugere af informationssystemer til at anvende systemer, der er i overensstemmelse med princippet om indbygget databeskyttelse.

88. Med hensyn til de eksterne aspekter af databeskyttelse anbefaler EDPS:

— at man i Stockholmprogrammet fremhæver betydningen af generelle aftaler med USA og andre tredjelande om databeskyttelse og dataudveksling,

([52]) Udtalelse fra EDPS af 19. december 2008 om meddelelse fra Kommissionen — På vej mod en EU-strategi for e-justice (EUT C 128 af 6.6.2009, s. 13).

— at respekten for grundlæggende rettigheder og især databeskyttelse aktivt fremmes, i forbindelse med tredjelande og med internationale organisationer,

— at man i Stockholmprogrammet omtaler, at udveksling af personoplysninger med tredjelande fordrer et tilstrækkeligt beskyttelsesniveau eller andre passende garantier i de pågældende tredjelande.

89. EDPS noterer sig med stor interesse udviklingen hen imod en EU-informationsstyringsstrategi og en europæisk informationsmodel og fremhæver, at der i disse projekter bør lægges vægt på databeskyttelseselementer, der skal uddybes i Stockholmprogrammet. Arkitekturen for udveksling af oplysninger bør bygge på »indbygget databeskyttelse« og »bedste tilgængelige teknikker«.

90. Den kendsgerning, at det er teknisk muligt at udveksle digital information mellem databaser, der kan samkøres, eller at flette disse databaser er ikke en begrundelse for en undtagelse fra princippet om formålsbegrænsning. Samkøring bør i konkrete tilfælde være baseret på klare og omhyggelige politiske valg. EDPS foreslår, at dette begreb præciseres i Stockholmprogrammet.

91. Anvendelse af personoplysninger, der er indsamlet i kommercielt øjemed, til retshåndhævelsesformål bør ifølge EDPS kun være muligt på strenge betingelser, der er præciseret i punkt 65 i denne udtalelse.

92. Andre forslag med hensyn til anvendelsen af personoplysninger omfatter:

— Opstilling af vægtige kriterier for valget mellem centrale og decentrale systemer og angivelse i Stockholmprogrammet af, at det er hensigten at opstille sådanne kriterier

— Indførelse af et elektronisk system for indrejse til og udrejse fra EU-medlemsstaternes område samt programmer for registrerede rejsende bør ikke omhandles i Stockholmprogrammet

— Støtte til en styrkelse af Europol og Eurojust og til den nye aftale, der for nylig er udarbejdet mellem Europol og Eurojust

— Opstilling af vægtige kriterier for anvendelsen af biometriske data, idet det sikres, at dataene kun anvendes, når det er nødvendigt, passende og står i rimeligt forhold til formålet, og når lovgiveren har godtgjort, at der er tale om udtrykkeligt angivne og legitime formål. Dna-oplysninger bør ikke anvendes, hvis den samme virkning kan opnås ved at anvende andre mindre følsomme oplysninger.

93. EDPS støtter e-justice og har fremsat nogle bemærkninger om, hvordan projektet kan forbedres (jf.punkt 83).

Udfærdiget i Bruxelles, den 10. juli 2009.

Peter HUSTINX

Europæisk Tilsynsførende for Databeskyttelse