DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE

Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om forslaget til Europa-Parlamentets og Rådets forordning om visuminformationssystemet (VIS) og udveksling af oplysninger mellem medlemsstaterne om visa til kortvarigt ophold (KOM(2004) 835 endelig)

(2005/C 181/06)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE HAR —

under henvisning til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 286,

under henvisning til Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 8,

under henvisning 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,

under henvisning 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, og

under henvisning til Kommissionens anmodning, modtaget den 25. januar 2005, om en udtalelse i overensstemmelse med artikel 28, stk. 2, i forordning (EF) nr. 45/2001 —

VEDTAGET FØLGENDE UDTALELSE:

1. **INDLEDNING**

1.1. **Indledende bemærkninger**

Etableringen af visuminformationssystemet (VIS) er et vigtigt led i EU's fælles visumpolitik og har været genstand for en række indbyrdes forbundne instrumenter.

— I april 2003 blev der på foranledning af Kommissionen foretaget en feasibility-undersøgelse af VIS ([1])

— I september 2003 foreslog Kommissionen at ændre en tidligere forordning om ensartet udformning af visa ([2]). Hovedformålet var at medtage biometriske data (ansigtsbillede og to fingeraftryk) i det nye visumformat. Disse biometriske data skulle lagres i en mikrochip.

([1]) Endelig rapport om visuminformationssystemet, bestilt af Kommissionen og udarbejdet af firmaet Trasys, april 2003.
([2]) KOM(2003) 558 endelig med 2003/0217 (CNS) og 2003/0218 (CNS).

— I juni 2004 gav en rådsbeslutning ([1]) startskuddet til opbygningen af visuminformationssystemet ved at fastsætte retsgrundlaget for at opføre det på EU's budget. Der blev med denne beslutning foreslået en central database med oplysninger i forbindelse med visumansøgninger, og der blev fastsat en udvalgsprocedure med henblik på at styre den tekniske udvikling af VIS.

I december 2004 vedtog Kommissionen et forslag til forordning om VIS og udveksling af oplysninger mellem medlemsstaterne om visa til kortvarigt ophold ([2]) (i det følgende benævnt »forslaget«), som denne udtalelse drejer sig om. Forslaget ledsages af en udvidet konsekvensanalyse ([3]).

Som det anføres i begrundelsen, vil der imidlertid i forlængelse af denne forordning være behov for yderligere retsakter om:

— ændring af de fælles konsulære instrukser til de diplomatiske og konsulære repræsentationer for de kontraherende parter i Schengen-konventionen (i det følgende benævnt »de fælles konsulære instrukser«) i forbindelse med indførelsen af biometriske data i procedurerne

— udvikling af en ny ordning for udveksling af oplysninger med Irland og Det Forenede Kongerige

— udveksling af oplysninger om visa til længerevarende ophold.

Som besluttet på samlingen i Rådet (retlige og indre anliggender) den 5.-6. juni 2003 og nærmere beskrevet i artikel 1, stk. 2, i ovennævnte rådsbeslutning fra juni 2004 baseres visuminformationssystemet på en centraliseret arkitektur med en database, hvor visumansøgningerne lagres: det centrale visuminformationssystem (CS-VIS) og en national grænseflade i hver medlemsstat (NI-VIS). Medlemsstaterne udpeger ([4]) en central national myndighed, der forbindes med den nationale grænseflade, og hvorigennem deres respektive kompetente myndigheder har adgang til CS-VIS.

1.2. **Forslagets hovedelementer med hensyn til databeskyttelse**

Forslaget tager sigte på at forbedre forvaltningen af den fælles visumpolitik ved at gøre det lettere at udveksle oplysninger mellem medlemsstaterne ved hjælp af en central database. Forordningen indebærer, at der indføres biometriske data (foto og fingeraftryk) i ansøgningsproceduren, og at disse data lagres i den centrale database.

Biometriske data kan også anvendes i forbindelse med visummærkaten, således som det bestemmes i Kommissionens forslag til forordning om ændring af forordningen om ensartet udformning af visa, således at der indføres foto og fingeraftryk, som lagres i en mikrochip (Rådet har endnu ikke truffet afgørelse herom, idet resultaterne af den igangværende analyse afventes).

Forslaget redegør nærmere for de forskellige former for behandling af oplysninger (indlæsning, ændring, sletning og søgning) og de forskellige oplysninger, der skal registreres i VIS, alt efter hvordan det er gået med ansøgningen (godkendelse, afslag, etc.)

I henhold til forslaget skal oplysningerne i forbindelse med hver enkelt ansøgning opbevares i fem år.

Forslaget anfører indskrænkende, hvilke andre kompetente myndigheder end visummyndighederne der skal have adgang til VIS, og fastlægger deres adgangsrettigheder:

— de myndigheder, som har kompetence til at foretage visumkontrol ved de ydre grænser og inden for medlemsstatens område

— de kompetente indvandringsmyndigheder

([1]) 2004/512/EF, EUT L 213 af 15.6.2004, s. 5.
([2]) KOM(2004) 835 endelig med 2004/0287 (COD).
([3]) Udvidet konsekvensanalyse af visuminformationssystemet, endelig rapport fra European Policy Evaluation Consortium, december 2004.
([4]) Artikel 24, stk. 2, i forslaget.

— de kompetence asylmyndigheder.

I beskrivelsen af VIS' drift og ansvarsområderne i den forbindelse understreger forslaget, at Kommissionen behandler oplysningerne i VIS på medlemsstaternes vegne. Det beskriver nødvendigheden af at oplysningerne anvendes på en sådan måde, at datasikkerheden garanteres, og angiver mere detaljeret det ansvar, de forskellige aktører har for at sikre et sådant sikkerhedsniveau.

Forslaget indeholder et kapitel om databeskyttelse, hvori de nationale myndigheders og Den Europæiske Tilsynsførende for Databeskyttelses rolle beskrives nærmere.

Forslaget overlader den tekniske gennemførelse af VIS og valget af de nødvendige teknologier til det udvalg, der er nedsat ved artikel 5, stk. 1, i forordning (EF) nr. 2424/2001 om udviklingen af anden generation af Schengen-informationssystemet (SIS II).

Forslaget ledsages af en udvidet konsekvensanalyse af VIS bestilt af Kommissionen og uarbejdet af European Policy Evaluation Consortium. Den konkluderer, at løsningen med et visuminformationssystem, der understøttes af biometriske data, er den bedste foreliggende metode til at forbedre den fælles visumpolitik.

2. **RELEVANTE RAMMER**

Forslaget vil i vid udstrækning gribe ind i fysiske personers privatliv og andre grundlæggende rettigheder. Det skal derfor kontrolleres i forhold til principperne om databeskyttelse. De vigtigste referencepunker for undersøgelsen omfatter følgende:

— Respekt for privatlivet har været sikret i Europa, lige siden Europarådet i 1950 vedtog konventionen til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder (i det følgende benævnt »EMRK«). Artikel 8 i EMRK omhandler »ret til respekt for privatliv og familieliv«.

  I henhold til artikel 8, stk. 2, må ingen offentlig myndighed må gøre indgreb i udøvelsen af denne ret, medmindre det sker »i overensstemmelse med loven« og er »nødvendigt i et demokratisk samfund« for at beskytte vigtige interesser. I Den Europæiske Menneskerettighedsdomstols retspraksis har disse betingelser ført til, at der er opstillet yderligere krav med hensyn til kvaliteten af retsgrundlaget for sådanne indgreb, foranstaltningernes proportionalitet og nødvendigheden af relevant beskyttelse mod misbrug.

  De grundlæggende principper for beskyttelse af fysiske personer i forbindelse med behandlingen af personoplysninger er opstillet i den konvention om databeskyttelse, som Europarådet udarbejdede og vedtog i 1981.

— Retten til respekt for privatliv og beskyttelse af personoplysninger er senere blevet fastlagt i artikel 7 og 8 i Den Europæiske Unions charter om grundlæggende rettigheder, som er indarbejdet i del II i den nye EU-forfatningstraktat.

  Ifølge charterets artikel 52 anerkendes det, at disse rettigheder kan begrænses på samme betingelser som dem, der gælder i henhold til artikel 8 i EMRK. Der skal ved vurderingen af ethvert forslag om eventuelle indgreb tages hensyn til disse betingelser.

I den nuværende EU-lovgivning er de grundlæggende regler om databeskyttelse fastlagt i:

— Europa-Parlamentet 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 (EFT L 281, s. 31). Dette direktiv benævnes i det følgende »direktiv 95/46/EF«. Direktivet indeholder nærmere principper, som forslaget skal kontrolleres i forhold til, for så vidt det skal finde anvendelse i medlemsstaterne. Dette er især relevant, eftersom forslaget skal anvendes sammen med den nationale lovgivning om direktivets gennemførelse. De foreslåede bestemmelser og beskyttelsesforanstaltningers effektivitet kommer derfor til at afhænge af, hvor effektiv denne kombination er i hvert enkelt tilfælde.

— 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 (EFT L 8, s.1). Denne forordning benævnes i det følgende »forordning nr. 45/2001«. Den indeholder principper, der svarer til principperne i direktiv 95/46/EF, og er relevant i denne sammenhæng, for så vidt forslaget skal finde anvendelse på Kommissionens aktiviteter, sammen med forordningens bestemmelser. Denne kombination skal derfor også vies nogen opmærksomhed.

Direktiv 95/46/EF og forordning nr. 45/2001 skal ses sammen med andre instrumenter. Med andre ord skal direktivet og forordningen, i det omfang de omhandler behandling af personoplysninger, der vil kunne krænke de grundlæggende frihedsrettigheder, navnlig retten til privatliv, fortolkes med udgangspunkt i de grundlæggende frihedsrettigheder. Dette følger også af EF-Domstolens retspraksis ([1]).

— Endelig vil Den Europæiske Tilsynsførende for Databeskyttelse også medtage udtalelse nr. 7/2004 af 11. august 2004 fra Gruppen vedrørende Beskyttelse af Personer i forbindelse med Behandling af Personoplysninger ([2]) om indførelse af biometriske elementer i opholdstilladelser og visa under hensyn til oprettelsen af det europæiske visuminformationssystem (VIS) i sin analyse. Gruppen gav i denne udtalelse udtryk for betænkeligheder ved en række elementer i forslaget. Den Europæiske Tilsynsførende for Databeskyttelse vil undersøge, hvorvidt og hvordan forslaget tager hensyn til disse betænkeligheder.

3. **ANALYSE AF FORSLAGET**

3.1. **Generelt**

Den Europæiske Tilsynsførende for Databeskyttelse erkender, at den videre udvikling af en fælles visumpolitik kræver en effektiv udveksling af relevante oplysninger. En af de mekanismer, der kan sikre en jævn informationsstrøm, er VIS. Et sådant nyt instrument bør imidlertid begrænses til indsamling og udveksling af oplysninger i det omfang, det er nødvendigt for at kunne udvikle en fælles visumpolitik og står i rimeligt forhold til denne målsætning.

Oprettelsen af VIS vil muligvis kunne få positive konsekvenser for andre legitime offentlige interesser, men dette ændrer ikke selve formålet med VIS. Systemets afgrænsede formål spiller en vigtig rolle med hensyn til at fastsætte systemets legitime indhold og anvendelse og dermed også for, hvordan medlemsstaternes myndigheder af hensyn til legitime offentlige interesser skal have adgang til VIS (eller dele af de deri indeholdte oplysninger).

Forslaget indfører desuden anvendelsen af biometriske data i VIS. Den Europæiske Tilsynsførende for Databeskyttelse erkender fordelene ved at anvende biometriske data, men understreger samtidig de omfattende virkninger af at anvende disse data og foreslår, at der indarbejdes strenge beskyttelsesforanstaltninger i forbindelse med anvendelsen af biometriske data.

Denne udtalelse skal ses på baggrund af disse overordnede overvejelser. Det bemærkes, at denne udtalelse bør nævnes i forordningens præambel før betragtningerne (»under henvisning til udtalelse ...«).

([1]) Det kan i denne forbindelse være nyttigt at henvise til Domstolens dom i Österreichischer Rundfunk m.fl. (forenede sager C-465/00, C-138/01 og C-139/01, dom af 20. maj 2003, Domstolens plenum, (2003) Sml. I-4989). Domstolen tog stilling til en østrigsk lov, der gjorde det muligt at videregive lønoplysninger om offentligt ansatte til den østrigske rigsrevision og derefter offentliggøre disse oplysninger. Domstolen opstiller i sin dom på baggrund af artikel 8 i den europæiske menneskerettighedskonvention en række kriterier, der skal gælde for anvendelsen af direktiv 95/46/EF, for så vidt dette direktiv tillader visse begrænsninger i retten til privatlivets fred.

([2]) Det er en uafhængig rådgivende gruppe bestående at repræsentanter for medlemsstaternes databeskyttelsesmyndigheder, Den Europæiske Tilsynsførende for Databeskyttelse og Kommissionen, som blev nedsat ved direktiv 95/46/EF.

3.2. **Formål**

Formålet med VIS er af afgørende betydning både set i lyset af såvel artikel 8 i EMRK og de generelle rammer for databeskyttelse. I henhold til artikel 6 i direktiv 95/46/EF skal personoplysninger »indsamles til udtrykkeligt angivne og legitime formål« og »senere behandling heraf ikke må være uforenelig med disse formål«. Kun med en klar definition af formålene vil det være muligt at foretage en korrekt vurdering af proportionaliteten og tilstrækkeligheden i behandlingen af personoplysninger, der er et omtåleligt spørgsmål pga. oplysningernes art (herunder biometriske data) og omfanget af den påtænke behandling af oplysningerne.

Formålet med VIS fremgår klart af forslagets artikel 1, stk. 2:

> »VIS forbedrer administrationen af den fælles visumpolitik, det konsulære samarbejde og konsultationerne mellem de centrale konsulære myndigheder ved at lette udvekslingen af oplysninger mellem medlemsstaterne om ansøgninger og om afgørelser i forbindelse hermed«.

Samtlige elementer i VIS skal derfor være nødvendige og forholdsmæssigt afstemte instrumenter til at nå dette politiske mål til fordel for den fælles visumpolitik.

Forslagets artikel 1, stk. 2, nævner også en række yderligere fordele ved at forbedre visumpolitikken, herunder bl.a.:

a) at forebygge trusler mod den indre sikkerhed

b) at lette bekæmpelsen af svig

c) at lette kontrollen ved kontrolstederne ved de ydre grænser.

Den Europæiske Tilsynsførende for Databeskyttelse ser disse elementer som eksempler på positive virkninger af at etablere VIS og af at forbedre den fælles visumpolitik, men ikke som selvstændige mål.

Dette indebærer to væsentlige konsekvenser på dette stadium:

— Den Europæiske Tilsynsførende for Databeskyttelse er klar over, at de retshåndhævende myndigheder er interesserede i at få adgang til VIS. Rådet vedtog konklusioner herom den 7. marts 2005. Eftersom formålet med VIS er at forbedre den fælles visumpolitik, skal det bemærkes, at det ikke vil være i overensstemmelse med dette formål at give de retshåndhævende myndigheder rutinemæssig adgang. Selv om der i henhold til artikel 13 i direktiv 95/46/EF kan gives ad hoc-adgang i visse tilfælde og med forbehold af de nødvendige garantier, kan der dog ikke tillades systematisk adgang.

  Mere generelt vil det være afgørende med en vurdering af proportionaliteten og nødvendigheden, hvis der i fremtiden skal træffes afgørelser om, hvorvidt visse andre myndigheder skal have adgang til VIS. De opgaver, i forbindelse med hvilke der gives adgang, skal være i overensstemmelse med visuminformationssystemets formål.

— Den udtrykkelige henvisning til »at forebygge trusler mod de enkelte medlemsstaters indre sikkerhed« i litra a) er uheldig. De vigtigste fordele ved VIS vil bestå i at forebygge svig og visum-shopping (bekæmpelse af svig er også hovedbegrundelsen for at medtage biometriske data i systemet) ([1]). Forebyggelse af trusler mod sikkerheden bør derfor ses som en sekundær, men dog yderst kærkommen fordel.

  Den Europæiske Tilsynsførende for Databeskyttelse anbefaler en mere udtrykkelig sondring mellem »formål« og »fordele« i artikel 1, stk. 2, f.eks. med følgende affattelse:

  > »VIS har til formål at forbedre administrationen af den fælles visumpolitik, det konsulære samarbejde og konsultationerne mellem de centrale konsulære myndigheder ved at lette udvekslingen af oplysninger mellem medlemsstaterne om ansøgninger og om afgørelser i forbindelse hermed. Det bidrager dermed også til …«.

([1]) Det siges meget klart i den udvidede konsekvensanalyse (s. 6, punkt 2.7), at *den manglende effektivitet i bekæmpelsen af visum-shopping og svig og i gennemførelsen af kontrol også skaber manglende effektivitet med hensyn til medlemsstaternes interne sikkerhed*. Dette antyder, at truslerne mod sikkerheden til dels skyldes en mangelfuld visumpolitik. Det første, der bør gøres i den forbindelse, er at forbedre visumpolitikken, især ved at bekæmpe svig og foretage en bedre kontrol. En bedre visumpolitik vil føre til en forbedring af sikkerheden.

Det skal i den forbindelse også bemærkes, at i de retningslinjer for indførelsen af et fælles system for udveksling af visumoplysninger, som RIA-Rådet vedtog den 13. juni 2002 ([1]), er forebyggelse af trusler mod den indre sikkerhed sat til sidst på listen. Det samme kunne gøres her og ville også være meget mere i overensstemmelse med visuminformationssystemets formål.

3.3. **Oplysningernes kvalitet**

I henhold til artikel 6 i direktiv 95/46/EF skal personoplysninger »være relevante og tilstrækkelige og ikke omfatte mere end, hvad der kræves til opfyldelse af de formål, hvortil de indsamles, og til de formål, hvortil de senere behandles«. Dette vedrører ikke kun proportionaliteten i selve visuminformationssystemet, men også de oplysninger, der skal indsamles og lagres i VIS, og deres videre anvendelse samt de supplerende beskyttelsesforanstaltninger i forbindelse hermed. Disse elementer er også væsentlige for vurderingen af forslaget på baggrund af artikel 8 i EMRK.

Etableringen af VIS udgør utvivlsomt et omfattende indgreb i udøvelsen af retten til respekt for privatlivet, om ikke andet så på grund af dets omfang og de former for personoplysninger, der skal behandles. Gruppen vedrørende Beskyttelse af Personer i forbindelse med Behandling af Personoplysninger bad derfor i sin udtalelse nr. 7/2004 om at få oplyst, hvilke undersøgelser af omfanget og grovheden af de pågældende fænomener der har vist, at tvingende årsager i forbindelse med den offentlige sikkerhed eller den offentlige orden kan retfærdiggøre en sådan løsning.

Den Europæiske Tilsynsførende for Databeskyttelse har nøje noteret sig den dokumentation, der forelægges i den udvidede konsekvensanalyse. Selv om denne dokumentation ikke er helt endegyldig, synes der at være berettiget grundlag for at oprette VIS for at forbedre den fælles visumpolitik.

Det forekommer i den forbindelse at ligge inden for lovgiverens skønsmargen at træffe afgørelse om at oprette VIS som et instrument, der skal forbedre vilkårene for medlemsstaternes visumudstedelse. Et sådant system vil i sig selv kunne passe ind i og understøtte den gradvise indførelse af et område med frihed, sikkerhed og retfærdighed som omhandlet i EF-traktaten.

Imidlertid må oprettelse og anvendelse af VIS aldrig få til følge, at der ikke længere kan sikres en høj grad af beskyttelse af personoplysninger på dette område. Det indgår i Den Europæiske Tilsynsførende for Databeskyttelses rådgivende opgaver at undersøge, i hvilket omfang VIS vil påvirke det eksisterende niveau for beskyttelse af oplysninger om de registrerede.

Den Europæiske Tilsynsførende for Databeskyttelse vil på denne baggrund fokusere på følgende spørgsmål i denne udtalelse:

— proportionaliteten og tilstrækkeligheden af oplysningerne og deres anvendelse (f.eks. kategorier af oplysninger, adgang til oplysninger for hver af de berørte myndigheder og lagringsperioden)

— systemets drift (f.eks. ansvarsfordeling og sikkerhed)

— de registreredes rettigheder (f.eks. oplysning og mulighed for at rette eller slette forkerte eller irrelevante oplysninger)

— overvågning af og kontrol med systemet.

Bortset fra nedenstående giver forslaget ikke anledning til væsentlige bemærkninger vedrørende de kategorier af oplysninger, der skal medtages i VIS, og deres anvendelse. De relevante bestemmelser er udarbejdet med behørig omhu og forekommer som helhed at være sammenhængende og tilstrækkelige.

([1]) Rådets rammeafgørelse af 13. juni 2002 om bekæmpelse af terrorisme (2002/475/RIA), EFT L 164 af 22.6.2002, s. 3.

3.4. **Biometriske data**

3.4.1. *Virkningerne af at anvende biometriske data*

Det er aldrig et uvæsentligt valg at anvende biometriske data i informationssystemer, navnlig når det pågældende system berører et meget stort antal enkeltpersoner. Biometriske data er ikke bare en ny informationsteknologi. De ændrer uigenkaldeligt forholdet mellem krop og identitet, idet de gør menneskekroppens karakteristika »maskinlæsbare« og til genstand for videre anvendelse. Selv om de biometriske egenskaber ikke kan læses med det menneskelige øje, kan de til enhver tid læses og anvendes ved hjælp af egnede værktøjer, uanset hvor den pågældende person tager hen.

Uanset hvor nyttige biometriske data kan være til nogle formål, vil udstrakt brug af dem imidlertid i høj grad påvirke samfundet og bør debatteres bredt og åbent. Den Europæiske Tilsynsførende for Databeskyttelse må konstatere, at der egentlig ikke har fundet en sådan debat sted, inden forslaget blev udarbejdet. Dette understreger i endnu højere grad, hvor nødvendigt det er med strenge beskyttelsesforanstaltninger i forbindelse med anvendelsen af biometriske data og med en grundig overvejelse og debat i lovgivningsforløbet.

3.4.2. *Særlige forhold i forbindelse med biometriske data*

Som allerede understreget i en række udtalelser fra Gruppen vedrørende Beskyttelse af Personer i forbindelse med Behandling af Personoplysninger ([1]) er det nødvendigt, at indførelse og behandling af biometriske data i forbindelse med identitetsrelaterede dokumenter omgives af særlig sammenhængende og strenge sikkerhedsforanstaltninger. Biometriske data er nemlig overordentlig følsomme på grund af en række særlige forhold.

Det er korrekt, at det er næsten umuligt for de berørte personer at miste de biometriske data, i modsætning til hvad der er tilfældet med et password eller en nøgle. De er *næsten 100 % distinktive*, dvs. at hver person har sine egne unikke biometriske data. De ændrer sig næsten aldrig i hele en persons levetid, og de karakteristiske egenskaber forbliver således *permanente*. Alle mennesker indeholder de samme fysiske »elementer«, således at de biometriske data også i et vist omfang bliver *universelle*.

Det er imidlertid næsten umuligt at slette biometriske data: det er vanskeligt at ændre en finger eller et ansigt. Denne positive egenskab har ud fra en række synspunkter en stor ulempe i forbindelse med *tyveri af identitet*: lagring af fingeraftryk og foto i en database sammen med en stjålet identitet vil kunne medføre store og varige problemer for identitetens rette ejer. Desuden er biometriske data ifølge sagens natur *ikke hemmelige* og kan endog *efterlade spor* (fingeraftryk, DNA), som gør det muligt at indsamle sådanne data, *uden at ejeren ved det*.

På grund af disse risici, som ligger i selve de biometriske datas natur, er det nødvendigt at iværksætte store beskyttelsesforanstaltninger (navnlig med hensyn til princippet om at begrænse indsatsen til det, der er nødvendigt for at nå det tilsigtede mål, begrænset adgang og sikkerhedsforanstaltninger).

3.4.3. *Tekniske mangler ved fingeraftryk*

De væsentligste fordele ved biometriske data er beskrevet ovenfor (deres egenskaber med hensyn til at være universelle, distinktive, permanente, anvendelige, osv.) er aldrig absolutte. Dette har direkte indvirkning på, hvor effektive den biometriske registrering og de kontrolprocedurer, der er planlagt i forordningen, bliver.

Det anslås ([2]) af op til 5 % af alle mennesker ikke vil kunne registreres (fordi de ikke har læsbare fingeraftryk eller slet ingen fingeraftryk). I den udvidede konsekvensanalyse, der ledsager forslaget, forventes det, at ca. 20 mio. mennesker vil søge om visum i 2007, hvilket betyder, at op til én million mennesker ikke vil kunne følge den »normale« registreringsprocedure, hvilket naturligvis får konsekvenser for visumansøgningen og grænsekontrollen.

([1]) Udtalelse nr. 7/2004 om indførelse af biometriske elementer i opholdstilladelser og visa under hensyn til oprettelsen af det europæiske visuminformationssystem (VIS) (Markt/11487/04/EN - WP 96) og arbejdsdokument om biometri (MARKT/10595/03/EN - WP 80).

([2]) A. Sasse, *Cybertrust and CrimePrevention: Usability and Trust in Information Systems*, i forbindelse med »Foresight cybertrust and crime prevention project«. 04/1151, 10. juni 2004, s. 7, og Technology Assessment, »Using Biometrics for Border Security«, United States General Accounting Office, GAO-03-174, november 2002.

Biometrisk identifikation er pr. definition også en statistisk proces. Det er normalt med en fejlprocent på mellem 0,5 og 1 % ([1]), hvilket betyder, at kontrolsystemet ved de ydre grænser vil få en fejlafvisningsfrekvens på mellem 0,5 og 1 %. Denne frekvens bestemmes af en tærskel, der er baseret på de kompetente myndigheders risikopolitik (den afspejler en afvejning mellem antallet af personer, der afvises fejlagtigt, og dem, der godkendes fejlagtigt). Det er derfor overdrevet at hævde, at disse teknologier vil give en »nøjagtig identifikation« af den registrerede som nævnt i betragtning 9 i forslaget til forordning.

Ifølge en nyere prospektiv undersøgelse ([2]) bestilt af Europa-Parlamentets Udvalg om Borgernes Friheder og Rettigheder og Retlige og Indre Anliggender bør der være *tilbagefaldsprocedurer*, der giver væsentlige garantier i forbindelse med indførelsen af biometriske data, da de hverken er tilgængelige for alle eller helt pålidelige. Der bør iværksættes og anvendes sådanne procedurer for at respektere værdigheden hos personer, der ikke har kunnet følge registreringsproceduren med gunstigt resultat, og for at undgå, at de belastes af manglerne ved systemet ([3]).

Den Europæiske Tilsynsførende for Databeskyttelse anbefaler derfor, at der udarbejdes tilbagefaldsprocedurer, som indarbejdes i forslaget. Disse procedurer bør hverken sænke sikkerhedsniveauet i visumpolitikken eller brændemærke personer med ulæselige fingeraftryk.

3.5. **Særlige kategorier af oplysninger**

Visse kategorier af oplysninger (foruden de biometriske data) kræver særlig opmærksomhed: oplysninger om grundene til afslag på visum (3.5.1) og oplysninger om andre gruppemedlemmer (3.5.2).

3.5.1. *Grunde til afslag på visum*

Forslagets artikel 10, stk. 2, indeholder bestemmelser om behandlingen af oplysninger om grundene til afslag, når der er truffet afgørelse om at give afslag på visum. Disse grunde til afslag er helt standardiserede.

— De to første grunde i litra a) og b) er nærmest af administrativ art: der er ikke fremlagt et gyldigt rejsedokument eller gyldige dokumenter, som beviser formålet med og betingelserne for det planlagte ophold.

— Litra c) henviser til, at »ansøgeren er indberettet som uønsket«, hvilket indebærer søgning i SIS-databasen.

— Endelig anføres der i litra d) som grund til at give afslag på visum, at ansøgeren »udgør en trussel mod en af medlemsstaternes offentlige orden, indre sikkerhed, folkesundhed eller internationale forbindelser«.

([1])

Biometri	Ansigt	Finger	Iris
FTE % registreringsfejl	uoplyst	4	7
FNMR % afvisning	4	2.5	6
FMR1 % verifikationsgenkendelsesfejl	10	< 0.01	< 0.001
FMR2 % identifikationsfejl ved en DB på > 1 m	40	0,1	uoplyst
FMR3 % screeningsgenkendelsesfejl ved en DB = 500	12	< 1	uoplyst

A. K. Jain et al., *Biometrics: A grand Challenge*, Proceedings of International Conference on Pattern Recognition, Cambridge, UK., August 2004

([2]) *Biometrics at the frontiers: assessing the impact on Society*, februar 2005, Instituttet for Teknologiske Fremtidsstudier, GD Det Fælles Forskningscenter, Europa-Kommissionen.

([3]) *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data*, Europarådet, 2005, side 11.

Alle grundene til afslag skal anvendes med største forsigtighed på grund af de følger, de har for den enkelte. Desuden vil nogle af dem, nemlig de grunde, der er nævnt i litra c) og d), føre til behandling af »følsomme oplysninger« som dem, der er nævnt i artikel 8 i direktiv 95/46/EF.

Den Europæiske Tilsynsførende for Databeskyttelse vil gerne i særlig grad henlede opmærksomheden på betingelsen vedrørende folkesundheden, der forekommer uprecis og indebærer behandling af meget følsomme oplysninger. Ifølge bemærkningerne til artiklerne i bilaget til forslaget bygger omtalen af trussel mod folkesundheden på »Forslag til Rådets forordning om indførelse af en fællesskabskodeks for personers passage af de fælles grænser« KOM(2004) 391 endelig.

Den Europæiske Tilsynsførende for Databeskyttelse er klar over, at kriteriet vedrørende »folkesundheden« i vid udstrækning bruges i fællesskabslovgivningen om fri bevægelighed for personer, og at det anvendes meget strengt, således som det fremgår af Europa-Parlamentets og Rådets direktiv 2004/38/EF af 29. april 2004 om unionsborgeres og deres familiemedlemmers ret til at færdes og opholde sig frit på medlemsstaternes område. Direktivets artikel 29 indeholder bestemmelser om, hvornår der skal tages hensyn til en trussel mod folkesundheden: »De eneste sygdomme, der kan begrunde foranstaltninger, der begrænser den frie bevægelighed, er de sygdomme, der er potentielt epidemiske ifølge relevante instrumenter fra Verdenssundhedsorganisationen, samt andre smitsomme infektionssygdomme eller parasitære sygdomme, for så vidt værtsmedlemsstaten har truffet beskyttelsesforanstaltninger mod dem for egne statsborgere.«

— Det skal imidlertid bemærkes, at det omtalte forslag indtil videre kun er et forslag, og at indførelse af kravet om ikke at udgøre en trussel mod folkesundheden i VIS-forordningen er betinget af, at der vedtages en fællesskabskodeks.

— Hvis forslaget vedtages, skal denne grund til afslag på indrejse desuden fortolkes indskrænkende. Faktisk bygger forslaget til fællesskabskodeks på ovennævnte direktiv 2004/38/EF.

Den Europæiske Tilsynsførende for Databeskyttelse anbefaler derfor, at der i forslaget indsættes en henvisning til artikel 29 i direktiv 2004/38/EF, for at sikre, at »trussel mod folkesundheden« forstås i overensstemmelse med denne bestemmelse. Under alle omstændigheder bør oplysningerne i betragtning af, hvor følsomme de er, kun behandles, hvis truslen mod folkesundheden er reel, aktuel og alvorlig.

3.5.2. *Oplysninger om andre gruppemedlemmer*

Artikel 2, stk. 7, definerer »gruppemedlemmer« som »andre ansøgere, som ansøgeren rejser sammen med, herunder ægtefælle og børn, som ledsager ansøgeren«. Det nævnes i bemærkningerne til artiklerne, at definitionerne i artikel 2 henviser til traktaten eller Schengen-reglerne om visumpolitik, bortset fra nogle enkelte udtryk, herunder »gruppemedlemmer«, der defineres specifikt med henblik på denne forordning. Det kan derfor antages, at denne definition ikke refererer til definitionen af »kollektivvisum« i punkt 2.1.4 i de fælles konsulære instrukser. Bemærkningerne til artiklerne nævner »ansøgere, som rejser i en gruppe sammen andre ansøgere, dvs. inden for rammerne af en aftale om status som godkendt destinationsland, eller sammen med familiemedlemmer«.

Den Europæiske Tilsynsførende for Databeskyttelse fremhæver, at forordningen bør indeholde en præcis og omfattende definition af »gruppemedlemmer«. Den Europæiske Tilsynsførende for Databeskyttelse bemærker, at definitionen er for uklar i det nuværende forslag, fordi der ikke er nogen præcis henvisning til traktaten eller Schengen-reglerne. Således som det er affattet, kunne »gruppemedlemmer« også omfatte kolleger, andre kunder i det samme rejsebureau, der deltager i en grupperejse, osv. Konsekvenserne heraf er faktisk ganske betydelige:

i henhold til artikel 5 i forslaget til forordning forbindes en persons ansøgningsdossier med de øvrige gruppemedlemmers ansøgningsdossierer.

3.6. **Lagring af oplysninger**

Det fastsættes i artikel 20 i forslaget til forordning, at hvert ansøgningsdossier lagres i fem år. Det er fællesskabslovgiveren, der træffer et politisk valg og fastsætter en rimelig tidsbegrænsning.

Der er navnlig i lyset af den begrundelse, der gives i bemærkningerne til artiklerne, ikke belæg for at hævde, at det politiske valg i forslaget er urimeligt, eller at det vil få uacceptable konsekvenser, forudsat at der indføres alle de nødvendige berigtigelsesmekanismer. Dette betyder, at det skal sikres, at oplysninger, der ikke længere er korrekte, berigtiges eller slettes, navnlig hvis en person har opnået statsborgerskab i en medlemsstat eller har fået en status, der ikke kræver, at vedkommende findes i systemet

Desuden må de data, der forsat ligger i systemet, på ingen måde foregribe en ny afgørelse. Nogle grunde til afslag (indberetning af en ansøger som uønsket og især trussel mod folkesundheden) har en begrænset tidsmæssig holdbarhed. Den omstændighed, at der på et givet tidspunkt har været gyldige grunde til nægtelse af indrejse, bør ikke have indflydelse på en ny afgørelse. Situationen skal tages op til fuldstændig nyvurdering i forbindelse med hver enkelt ny visumansøgning, og dette bør præciseres i forordningen, hvor det er relevant.

3.7. **Adgang til oplysninger og anvendelse af oplysninger**

3.7.1. *Indledende bemærkninger*

Som en indledende bemærkning anerkender Den Europæiske Tilsynsførende for Databeskyttelse den omhu, der tydeligvis er lagt i reglerne om adgang til og anvendelse af oplysningerne i VIS. Hver myndighed har adgang til forskellige oplysninger til forskellige formål. Det er en hensigtsmæssige fremgangsmåde, som Den Europæiske Tilsynsførende for Databeskyttelse kun kan tilskynde til. Bemærkningerne i det følgende tager sigte på at anvende denne fremgangsmåde i videst muligt omfang.

3.7.2. *Kontrol af visa ved de ydre grænser og inden for medlemsstatens område*

For så vidt angår kontrol af visa ved de ydre grænser nævner artikel 16 i forslaget til forordning to konkrete formål:

— »at verificere personens identitet«, hvilket i henhold til den givne definition indebærer en sammenligning punkt for punkt

— »at verificere visummets ægthed«. Som foreslået i ICAO-standarderne kan mikrochippen i visummet anvende offentlige/private nøglepar (PKI) til denne autentificering.

Begge disse formål kan opfyldes på passende måde, hvis de myndigheder, der har kompetence til at kontrollere visa, kun får adgang til den beskyttede mikrochip. Det vil derfor i dette konkrete tilfælde være for vidtgående at give adgang til den centrale VIS-database. Sidstnævnte mulighed ville betyde, at flere myndigheder skulle kobles på VIS, hvorved faren for misbrug ville blive større. Det ville måske også blive dyrere, da hyppigheden af sikker og kontrolleret adgang til VIS samt behovet for særlig uddannelse vedrørende denne adgang også ville vokse betydeligt.

Der er desuden tvivl om, hvorvidt den adgang til oplysninger, der er nævnt i artikel 16, stk. 2, er tilstrækkelig. Det fremgår nemlig af stk. 2, litra a), at hvis den første søgning viser, at der er registreret oplysninger om ansøgeren i VIS (hvilket i princippet bør være tilfældet), kan den kompetente myndighed konsultere andre oplysninger ligeledes med henblik på at verificere identiteten. Disse data omfatter alle oplysninger i tilknytning til ansøgningen, fotografier, fingeraftryk og oplysninger om visa, som tidligere er udstedt, annulleret, inddraget eller forlænget.

Hvis det er lykkedes at verificere identiteten, står det hen i det uvisse, hvorfor det fortsat er nødvendigt med de øvrige oplysninger. Der bør egentlig kun være adgang til dem, og det på restriktive vilkår, hvis verifikationsprocedurerne ikke har givet noget positivt resultat. I så fald vil de oplysninger, der er nævnt i artikel 16, stk. 2, på passende måde bidrage til en tilbagefaldsprocedure, der gør det lette at fastslå personens identitet. Der bør derfor ikke være adgang til dem for hele personalet ved grænsekontrolstederne, men blot i mere begrænset omfang for de embedsmænd, der har ansvaret for behandlingen af vanskelige sager.

Endelig bør definitionen af, hvilke myndigheder der har adgang, gøres tydeligere. Navnlig er det uklart, hvem de »myndigheder, som har kompetence til at foretage kontrol inden for medlemsstatens område«, er. Den Europæiske Tilsynsførende for Databeskyttelse antager, at det drejer sig om de myndigheder, som har kompetence til at foretage kontrol af visa, og artikel 16 bør ændres i overensstemmelse hermed.

3.7.3. *Anvendelse af oplysninger til identifikation og tilbagesendelse af ulovlige indvandrere og i asylprocedurer*

I de tilfælde, der er beskrevet i artikel 17, 18 og 19 (tilbagesendelse af ulovlige indvandrere og asylprocedure), anvendes VIS til identifikation. En af de former for oplysninger, der kan anvendes til identifikation, er fotografier. Imidlertid er det med den nuværende teknologi inden for automatisk ansigtsgenkendelse i så store it-systemer ikke muligt at anvende fotografier til identifikation (en-til-mange), idet de ikke kan give noget pålideligt resultat. De anses derfor ikke for at være tilstrækkelige oplysninger til identifikation.

Den Europæiske Tilsynsførende for Databeskyttelse henstiller derfor på det kraftigste til at lade »fotografier« udgå i første del af disse artikler og bibeholde dem i anden del (fotografier kan anvendes som et redskab til at verificere en persons identitet, men ikke til at identificere personer i en stor database).

En anden løsning kunne bestå i at ændre artikel 36, således at funktionerne for behandling af fotografier med henblik på identifikation først gennemføres, når teknologien skønnes at være pålidelig (eventuelt efter udtalelse fra det tekniske udvalg).

3.7.4. *Offentliggørelse af listerne over myndigheder med adgang*

I henhold til artikel 4 i forslaget til forordning offentliggøres listerne over de kompetente myndigheder, der er udpeget i hver medlemsstat med henblik på adgang til VIS, i *Den Europæiske Unions Tidende*. Offentliggørelsen bør være regelmæssig (årlig) for at oplyse om ændringer i de nationale forhold. Den Europæiske Tilsynsførende for Databeskyttelse understreger, at en sådan offentliggørelse er vigtig som et uundværligt kontrolredskab på såvel europæisk som nationalt og lokalt plan.

3.8. **Ansvar**

Der skal her erindres om, at VIS baseres på en centraliseret arkitektur med en central database, hvor alle visuminformationer lagres, og nationale grænseflader i medlemsstaterne, hvor medlemsstaternes kompetente myndigheder kan få adgang til det centrale system. Ifølge betragtning 14 og 15 i forslaget til forordning finder direktiv 95/46/EF anvendelse på medlemsstaternes behandling af personoplysninger i medfør af denne forordning, og forordning nr. 45/2001 finder anvendelse på Kommissionens aktiviteter med hensyn til beskyttelse af personoplysninger. Som nævnt i disse betragtninger i denne forbindelse tager forslaget sigte på at præcisere visse punkter bl.a. hvad angår ansvaret for anvendelsen af oplysninger og tilsyn med databeskyttelsen.

Disse punkter forekommer faktisk at vedrøre nogle afgørende detaljer, som, hvis de ikke var til stede, ville betyde, at garantierne i direktiv 95/46/EF og forordning nr. 45/2001 ikke ville finde anvendelse eller ikke være helt i overensstemmelse med forslaget. Anvendelsen af national ret i henhold til direktivet kræver almindeligvis, at der er etableret en registeransvarlig i den pågældende medlemsstat (artikel 4), medens forordningens anvendelse forudsætter, at behandlingen af personoplysninger finder sted i en fællesskabsinstitution eller et fællesskabsorgan som led i udøvelsen af aktiviteter, der helt eller delvis hører under fællesskabsrettens anvendelsesområde (artikel 3).

Det hedder i artikel 23, stk. 2, i forslaget til forordning, at oplysningerne »behandles af VIS på medlemsstaternes vegne«. I henhold til artikel 23, stk. 3, udpeger hver medlemsstat den myndighed, som skal betragtes som registeransvarlig efter artikel 2, litra d), i direktiv 95/46/EF. Dette tyder på, at Kommissionen ifølge ordningen i direktivet skal betragtes som registerfører. Dette underbygges af bemærkningerne til artiklerne ([1]).

Denne affattelse underspiller i nogen grad Kommissionens meget vigtige og endog afgørende rolle både i systemets udviklingsfase og i dets normale drift. Det er vanskelig at foretage en præcis sammenkædning mellem Kommissionens rolle med funktionen som registeransvarlig eller registerfører. Den er enten registerfører med usædvanlige beføjelser (bl.a. i forbindelse med udformningen af systemet) eller registeransvarlig med begrænsninger (eftersom oplysningerne indlæses og anvendes af medlemsstaterne). Kommissionen har faktisk en form for sui generis-rolle ([2]) i VIS.

Denne vigtige rolle bør anerkendes med en omfattende beskrivelse af Kommissionens opgaver, frem for at der anvendes en affattelse, der ikke helt svarer til virkeligheden, fordi den er for restriktiv, ikke ændrer noget i driften af VIS og kun bidrager til at skabe forvirring. Dette er også vigtigt af hensyn til et konsekvent og effektivt tilsyn med VIS (jf. også punkt 3.11). Den Europæiske Tilsynsførende for Databeskyttelse anbefaler derfor, at artikel 23, stk. 2, udgår.

Den Europæiske Tilsynsførende for Databeskyttelse vil gerne fremhæve, at det er ekstra vigtigt med en fuldstændig beskrivelse af Kommissionens opgaver i forbindelse med VIS, hvis Kommissionen påtænker at uddelegere forvaltningsopgaverne til et andet organ. Det fremgår af finansieringsoversigten til forslaget, at det vil være muligt at uddelegere disse opgaver til Det Europæiske Grænseagentur. Det er i den forbindelse overordentlig vigtigt, at Kommissionen ikke efterlader nogen usikkerhed med hensyn til rækkevidden af dens beføjelser, således at dens efterfølger kan vide, inden for hvilke rammer vedkommende kan handle.

3.9. **Sikkerhed**

Forvaltning og overholdelse af et optimalt sikkerhedsniveau i VIS er en nødvendig forudsætning for at sikre den krævede beskyttelse af de personoplysninger, der lagres i VIS-databasen. For at opnå et sådant tilfredsstillende beskyttelsesniveau er det nødvendigt at iværksætte passende beskyttelsesforanstaltninger for at håndtere de mulige risici i forbindelse med systemets infrastruktur og de berørte personer. Dette spørgsmål tages nu op i forskellige dele af forslaget og bør forbedres yderligere.

Forslagets artikel 25 og 26 indeholder en række foranstaltninger vedrørende datasikkerhed og anfører, hvilke former for misbrug der skal undgås. Det vil imidlertid være nyttigt at supplere disse bestemmelser med foranstaltninger til systematisk kontrol og indberetning af, hvor effektive de allerede nævnte sikkerhedsforanstaltninger er. Den Europæiske Tilsynsførende for Databeskyttelse anbefaler mere konkret, at der til disse artikler føjes bestemmelser om systematisk (egen)kontrol af sikkerhedsforanstaltningerne.

Dette er knyttet til forslagets artikel 40 om kontrol og evaluering. Dette bør ikke kun vedrøre resultater, omkostningseffektivitet og tjenesternes kvalitet, men også overholdelsen af de lovbestemte krav, navnlig med hensyn til databeskyttelse. Den Europæiske Tilsynsførende for Databeskyttelse anbefaler derfor, at anvendelsesområdet for artikel 40 udvides til også at omfatte kontrol og indberetning af behandlingens lovlighed.

Det bør desuden som supplement til artikel 24, stk. 4, litra c), eller artikel 26, stk. 2, litra e), om behørigt bemyndigede medarbejdere, der har adgang til oplysningerne, tilføjes, at medlemsstaterne skal sikre, at der foreligger præcise brugerprofiler (som de nationale tilsynsmyndigheder har adgang til med henblik på kontrol). Foruden disse brugerprofiler skal medlemsstaterne opstille og løbende ajourføre en fuldstændig liste over brugernes identitet. Det samme gælder Kommissionen. Artikel 25, stk. 2, litra b), bør derfor suppleres tilsvarende.

([1]) Jf. forslaget, s. 37.

([2]) Definitionen af registeransvarlig i direktiv 95/46/EF og forordning nr. 45/2001 giver dog også mulighed for at have flere registeransvarlige med forskellige ansvarsområder.

Disse sikkerhedsforanstaltninger suppleres med kontrol og organisatorisk beskyttelse. Forslagets artikel 28 beskriver de vilkår og formål, der skal gælde for førelse af registre over alle behandlinger af oplysninger. Registrene skal lagres ikke blot med henblik på kontrol i databeskyttelsesøjemed og til at garantere oplysningernes sikkerhed, men også med henblik på regelmæssig egenkontrol af VIS. Egenkontrolrapporterne vil bidrage til den effektive gennemførelse af tilsynsmyndighedernes opgaver, så disse myndigheder kan indkredse de største svagheder og koncentrere sig om dem i deres egen kontrolprocedure.

3.10. **Registreredes rettigheder**

3.10.1. *Underretning af registrerede*

Det er af allerstørste betydning, at registrerede underrettes, så der sikres en retfærdig sagsbehandling. Dette er en helt nødvendig beskyttelse af fysiske personers rettigheder. Forslagets artikel 30 følger nu i store træk artikel 10 i direktiv 95/46/EF for så vidt angår dette spørgsmål.

Dette ville imidlertid være gavnligt at foretage en række ændringer i denne bestemmelse, så den kommer til at passe bedre ind i rammerne for VIS. Direktivet nævner faktisk visse oplysninger, der skal gives, men giver også mulighed for yderligere information, hvis det er relevant ([1]). Artikel 30 bør derfor ændres til også at omfatte følgende:

— De registrerede bør også underrettes om, hvor længe deres oplysninger opbevares.

— Artikel 30, stk. 1, litra e), vedrører »ret til at få indsigt i og foretage berigtigelse af oplysningerne«. Det ville være mere korrekt at tale om »ret til at få indsigt i oplysningerne og ret til at *begære* dem berigtiget eller *slettet*«. De registrerede bør i den forbindelse oplyses om, at de kan søge råd eller bistand hos de relevante tilsynsmyndigheder.

— Endelig nævnes der i artikel 30, stk. 1, litra a), oplysninger om identiteten af den registeransvarlige og eventuelt af dennes repræsentant. Da den registeransvarlige altid er etableret på Den Europæiske Unions område, er det ikke nødvendigt at medtage sidstnævnte mulighed.

3.10.2. *Ret til indsigt og berigtigelse og sletning af oplysninger*

Det hedder i artikel 31, stk. 1, sidste punktum, at »det er kun en medlemsstat, der kan give adgang til oplysningerne«. Der er grund til at antage, at dette betyder, at en hvilken som helst medlemsstat, men ikke den centrale enhed, kan give adgang til (eller videregive) oplysninger. Den Europæiske Tilsynsførende for Databeskyttelse anbefaler, at det nævnes udtrykkeligt, at der kan anmodes om sådanne oplysninger i enhver medlemsstat.

Affattelsen af denne bestemmelse synes også at indebære, at der ikke kan gives afslag på indsigt, og at der gives indsigt uden godkendelse fra den ansvarlige medlemsstat. Dette forklarer, hvorfor de nationale myndigheder skal samarbejde om håndhævelsen af rettighederne i artikel 31, stk. 2, 3 og 4, men ikke artikel 31, stk. 1 ([2]).

3.10.3. *Bistand fra tilsynsmyndighederne*

Det fastsættes i artikel 33, stk. 2, at de nationale tilsynsmyndigheders pligt til at bistå og rådgive den pågældende gælder under hele processen (ved en domstol). Det står ikke helt klart, hvad der menes med dette stykke. De nationale tilsynsmyndigheder har forskellige holdninger til deres rolle i en retssag. Dette lyder, som om de skal fungere som rådgiver for klager i retten, hvilket i mange lande ikke er muligt.

([1]) Artiklen omhandler *»alle yderligere informationer (…) for så vidt som disse yderligere informationer, under hensyn til de særlige omstændigheder hvorunder oplysningerne indsamles, er nødvendige for at sikre den registrerede en rimelig behandling af oplysningerne«.*

([2]) Artikel 31, stk. 3, vedrørende samarbejde mellem de nationale myndigheder om retten til berigtigelse og sletning kunne derfor tydeliggøres således: »Hvis *den i stk. 2 omhandlede* anmodning«. Anmodninger i henhold til artikel 31, stk. 1, (adgang) indebærer ikke samarbejde mellem myndighederne.

3.11. **Tilsyn**

Forslaget fordeler tilsynsopgaven mellem de nationale tilsynsmyndigheder og Den Europæiske Tilsynsførende for Databeskyttelse. Dette er i tråd med forslagets tilgang til gældende ret og ansvaret for drift og anvendelse af VIS og med behovet for et effektivt tilsyn. Den Europæiske Tilsynsførende for Databeskyttelse ser derfor med tilfredshed på denne fremgangsmåde i artikel 34 og 35.

De nationale tilsynsmyndigheder overvåger, at medlemsstaternes behandling af personoplysninger, *herunder fremsendelsen af oplysningerne til og fra VIS*, foregår på lovlig vis. Den Europæiske Tilsynsførende for Databeskyttelse overvåger Kommissionens aktiviteter *(…), herunder at personoplysningerne fremsendes på lovlig vis mellem de nationale grænseflader og det centrale visuminformationssystem*. Dette vil eventuelt kunne føre til overlapning, eftersom både den nationale tilsynsmyndighed og Den Europæiske Tilsynsførende for Databeskyttelse på en og samme tid har ansvaret for at overvåge, at personoplysningerne fremsendes på lovlig vis mellem de nationale grænseflader og det centrale visuminformationssystem.

Den Europæiske Tilsynsførende for Databeskyttelse foreslår derfor, at artikel 34 ændres for at præcisere, at de nationale tilsynsmyndigheder overvåger, at medlemsstaternes behandling af personoplysninger, herunder fremsendelsen af oplysningerne til og fra den nationale VIS-grænseflade, foregår på lovlig vis.

Det er i forbindelse med tilsynet med VIS også vigtigt at understrege, at, at de nationale tilsynsmyndigheders og Den Europæiske Tilsynsførende for Databeskyttelses tilsynsvirksomhed i et vist omfang bør samordnes for at sikre en tilstrækkelig grad af konsekvens og samlet effektivitet. Der er således behov for en harmoniseret gennemførelse af forordningen og for at arbejde hen imod en fælles tilgang til fælles problemer. Det kan desuden tilføjes, at sikkerhedsniveauet i VIS sidste ende afhænger af sikkerheden i systemets svageste led. Det er i den forbindelse også nødvendigt at strukturere og forstærke samarbejdet mellem Den Europæiske Tilsynsførende for Databeskyttelse og de nationale myndigheder. Artikel 35 bør derfor indeholde en bestemmelse om, at Den Europæiske Tilsynsførende for Databeskyttelse indkalder til møde med samtlige nationale tilsynsmyndigheder mindst én gang om året.

3.12. **Gennemførelse**

Det hedder i forslagets artikel 36, stk. 2, at »*De foranstaltninger, som er nødvendige for den tekniske gennemførelse af de funktioner, der er omhandlet i stk. 1, vedtages efter proceduren i artikel 39, stk. 2.*« Artikel 39 omhandler et udvalg, der skal bistå Kommissionen, og som blev nedsat i december 2001 ([1]) og har været anvendt i en række instrumenter.

Den tekniske gennemførelse af funktionerne i VIS (samspillet med de kompetente myndigheder og ensartet udformning af visa) kan på en række potentielt kritiske punkter påvirke databeskyttelsen. For eksempel vil valgmulighederne med hensyn til, om visummet skal indeholde en mikrochip eller ej, påvirke anvendelsen af den centrale database, ligesom det standardformat, der anvendes til udveksling af biometriske data, kommer til at styre eller forme den dertil knyttede databeskyttelsespolitik ([2]).

Valget af teknologi får afgørende indflydelse på en korrekt gennemførelse af principperne om formål og proportionalitet, og bør følgelig være omfattet af tilsyn. Teknologivalg, der i væsentligt omfang påvirker databeskyttelsen, bør derfor fortrinsvis træffes gennem en forordning efter den fælles beslutningsprocedure. Kun på den måde er det muligt at sikre den nødvendige politiske kontrol. I alle andre tilfælde, hvor databeskyttelsen påvirkes, bør Den Europæiske Tilsynsførende for Databeskyttelse have mulighed for at udtale sig om de valg, udvalget træffer.

3.13. **Interoperabilitet**

Interoperabilitet er en kritisk og afgørende forudsætning for effektiviteten i store edb-systemer som VIS. Den gør det muligt at begrænse de samlede udgifter på en sammenhængende måde og undgå naturlige overlapninger af heterogene elementer. Interoperabilitet kan også bidrage til målsætningen om en fælles visumpolitik ved at anvende den samme proceduremæssige standard på alle de elementer, der indgår i denne politik. Det er imidlertid afgørende, at der sondres mellem to interoperabilitetsniveauer:

— Interoperabilitet mellem EU's medlemsstater er særdeles ønskelig, og f.eks. er det nødvendigt, at visumansøgninger, der fremsendes fra en medlemsstats myndigheder, er interoperable med dem, der fremsendes fra en hvilken som helst anden medlemsstats myndigheder.

([1]) Rådets forordning (EF) nr. 2424/2001 af 6. december 2001 om udviklingen af anden generation af Schengen-informationssystemet (SIS II).

([2]) Forslag til Rådets forordning om ændring af forordning (EF) nr. 1683/95 (om ensartet udformning af visa) fra september 2003 indeholdt også en tilsvarende artikel.

— Der kan i langt højere grad sættes spørgsmålstegn ved interoperabilitet mellem systemer, der er konstrueret til forskellige formål eller med systemer i tredjelande.

Af de tilgængelige beskyttelsesforanstaltninger, der anvendes til at begrænse systemets formål og forebygge »funktionsskred«, er anvendelsen af forskellige teknologistandarder en af dem, der kan bidrage til denne begrænsning. Desuden bør enhver form for interaktion mellem to forskellige systemer være veldokumenteret. Interoperabilitet må aldrig føre til en situation, hvor en myndighed, der ikke har ret til at få indsigt i eller anvende visse oplysninger, kan skaffe sig adgang til dem gennem et andet informationssystem.

Den Europæiske Tilsynsførende for Databeskyttelse vil i den forbindelse gerne henvise til Det Europæiske Råds erklæring af 25. marts 2004 om bekæmpelse af terrorisme, hvori Kommissionen opfordres til at forelægge forslag med henblik på forbedret interoperabilitet og synergier mellem informationssystemer (SIS, visuminformationssystemet og Eurodac).

Han vil også gerne henvise til de igangværende drøftelser om, hvilket organ der i fremtiden vil kunne få overdraget opgaven med at forvalte de forskellige store systemer (jf. også punkt 3.8 i denne udtalelse).

Den Europæiske Tilsynsførende for Databeskyttelse fremhæver på ny, at interoperabilitet mellem systemerne ikke må gennemføres, hvis det krænker princippet om begrænsning af formålet, og at ethvert forslag herom bør forelægges ham.

4. **KONKLUSIONER**

4.1. **Generelt**

1. Den Europæiske Tilsynsførende for Databeskyttelse erkender, at det for at videreudvikle en fælles visumpolitik er nødvendigt med en effektiv udveksling af relevante oplysninger. En af de mekanismer, der kan sikre en gnidningsløs informationsstrøm, er VIS. Den Europæiske Tilsynsførende for Databeskyttelse har nøje noteret sig den dokumentation, der forelægges i den udvidede konsekvensanalyse. Selv om denne dokumentation ikke er helt endegyldig, synes der at være berettiget grundlag for at oprette VIS for at forbedre den fælles visumpolitik.

   Det nye instrument bør imidlertid begrænses til indsamling og udveksling af oplysninger i det omfang, det er nødvendigt for at kunne udvikle en fælles visumpolitik og står i rimeligt forhold til denne målsætning.

2. Oprettelsen af VIS vil muligvis kunne få positive konsekvenser for andre legitime offentlige interesser, men dette ændrer ikke selve formålet med VIS. Samtlige elementer i VIS skal derfor være nødvendige og forholdsmæssigt afstemte instrumenter til at nå ovennævnte politiske mål.

   Endvidere:

   — vil det ikke være i overensstemmelse med dette formål at give de retshåndhævende myndigheder rutinemæssig adgang.

   — anbefaler Den Europæiske Tilsynsførende for Databeskyttelse en mere udtrykkelig sondring mellem »formål« og »fordele« i artikel 1, stk. 2

   — må interoperabilitet mellem systemerne ikke gennemføres, hvis det krænker princippet om begrænsning af formålet.

3. Den Europæiske Tilsynsførende for Databeskyttelse erkender fordelene ved at anvende biometriske data, men understreger samtidig de omfattende virkninger af at anvende disse data og foreslår, at der indarbejdes strenge beskyttelsesforanstaltninger i forbindelse med anvendelsen af biometriske data. Desuden gør de tekniske mangler ved fingeraftryk det nødvendigt, at der udarbejdes tilbagefaldsprocedurer, som indarbejdes i forslaget.

4. Denne udtalelse bør nævnes i forordningens præambel før betragtningerne (»under henvisning til udtalelse ...«).

4.2. **Andet**

5. Vedrørende grunde til afslag på visum: der bør i forslaget indsættes en henvisning til artikel 29 i direktiv 2004/38/EF, for at sikre, at »trussel mod folkesundheden« forstås i overensstemmelse med denne bestemmelse.

6. Oplysninger om gruppemedlemmer har særlig betydning i dette forslag. Der bør derfor gives en præcis og omfattende definition af »gruppemedlemmer«.

7. Der er ikke belæg for at hævde, at det politiske valg i forslaget med hensyn til, hvor længe oplysningerne skal opbevares, er urimeligt, eller at det vil få uacceptable konsekvenser, forudsat at der indføres alle de nødvendige berigtigelsesmekanismer.

   Det bør desuden nævnes udtrykkeligt i forslaget, at personoplysningerne skal tages op til fuldstændig nyvurdering i forbindelse med hver enkelt ny visumansøgning.

8. Vedrørende visumkontrol ved de ydre grænser: forslagets artikel 16 bør ændres, da det i disse tilfælde vil være for vidtgående at give adgang til den centrale VIS-database. Det vil være tilstrækkeligt, hvis de myndigheder, der har kompetence til at kontrollere visa, kun får adgang til den beskyttede mikrochip.

   Det står det hen i det uvisse, hvorfor det fortsat er nødvendigt med de øvrige oplysninger, hvis det er lykkedes at verificere identiteten.

9. Vedrørende anvendelse af oplysninger til identifikation og tilbagesendelse af ulovlige indvandrere og i asylprocedurer: »fotografier« bør udgå i første del af artikel 17, 18 og 19 og bibeholdes i anden del.

10. Vedrørende Kommissionens og medlemsstaternes ansvar: artikel 23, stk. 2, bør udgå.

11. Forslaget bør suppleres med bestemmelser om systematisk (egen)kontrol af sikkerhedsforanstaltningerne. Anvendelsesområdet for artikel 40 skal udvides til også at omfatte kontrol og indberetning af behandlingens lovlighed. Endvidere:

   — skal medlemsstaterne opstille og løbende ajourføre en fuldstændig liste over brugernes identitet. Det samme gælder Kommissionen. Artikel 25, stk. 2, litra b), bør derfor suppleres tilsvarende.

   — beskriver forslagets artikel 28 de vilkår og formål, der skal gælde for førelse af registre over alle behandlinger af oplysninger. Registrene skal lagres ikke blot med henblik på kontrol i databeskyttelsesøjemed og til at garantere oplysningernes sikkerhed, men også med henblik på regelmæssig egenkontrol af VIS.

12. Vedrørende registreredes rettigheder

   — Artikel 30 bør ændres, så det sikres, at de registrerede også informeres om, hvor længe oplysningerne om dem vil blive opbevaret.

   — Artikel 30, stk. 1, litra e), bør nævne »ret til at få indsigt i oplysningerne om vedkommende og ret til at begære dem berigtiget eller slettet«.

   — Artikel 31, stk. 1, skal præcisere, at der kan anmodes om visse oplysninger i enhver medlemsstat.

13. Vedrørende tilsyn

— Artikel 34 bør ændres for at præcisere, at de nationale tilsynsmyndigheder overvåger, at medlemsstaternes behandling af personoplysninger, herunder fremsendelsen af oplysningerne til og fra den nationale VIS-grænseflade, foregår på lovlig vis.

— Artikel 35 bør derfor indeholde en bestemmelse om, at Den Europæiske Tilsynsførende for Databeskyttelse indkalder til møde med samtlige nationale tilsynsmyndigheder mindst én gang om året.

14. Vedrørende gennemførelse

— Teknologivalg, der i væsentligt omfang påvirker databeskyttelsen, bør fortrinsvis træffes gennem en forordning efter den fælles beslutningsprocedure.

— I andre tilfælde bør Den Europæiske Tilsynsførende for Databeskyttelse have mulighed for at udtale sig om de valg, som det i forslaget omhandlede udvalg træffer.

Udfærdiget i Bruxelles, den 23. marts 2005

Den Europæiske Tilsynsførende for Databeskyttelse

Peter HUSTINX