

EUROPEISKA DATATILLSYNSMANNEN

Yttrande från Europeiska datatillsynsmannen om förslaget till Europaparlamentets och rådets förordning om ändring av de gemensamma konsulära anvisningarna angående viseringar till diplomatiska beskickningar och karriärkonsulat i samband med införandet av biometri samt bestämmelser om organiseringen av mottagandet och behandlingen av viseringsansökningar (KOM (2006) 269 slutlig) — 2006/0088 (COD)

(2006/C 321/14)

EUROPEISKA DATATILLSYNSMANNEN HAR ANTAGIT DETTA YTTRANDE

med beaktande av fördraget om upprättandet av Europeiska gemenskapen, särskilt artikel 286,

med beaktande av Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artikel 8,

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter,

med beaktande av Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter, och särskilt artikel 41,

med beaktande av kommissionens begäran om ett yttrande i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 som mottogs den 19 juni 2006.

HÄRIGENOM FRAMFÖRS FÖLJANDE.

1. INLEDNING

Den föreslagna förordningen har två huvudsakliga mål, båda i syfte att genomföra Informationssystemet för viseringar;

- Att tillhandahålla en rättslig grund för medlemsstaterna att uppta obligatoriska biometriska kännetecken från viseringssökande,
- att tillhandahålla en rättslig ram för hur medlemsstaternas konsulat skall organiseras, särskilt genom att organisera ett eventuellt samarbete mellan medlemsstaterna för behandlingen av viseringsansökningar.

Dessa två mål ger upphov till olika frågor när det gäller dataskydd och kommer att behandlas i skilda punkter, trots att de utgör en del av samma förslag.

Det aktuella förslaget syftar till att ändra de gemensamma konsulära anvisningarna. Dessa antogs av verkställande kommittén, som inrättades genom konventionen om tillämpning av Schengenavtalet av den 14 juni 1985. Som en del av Schengenregelverket införlivades de i EU-lagstiftningen genom ett protokoll fogat till Amsterdamfördraget, och har ändrats flera gånger sedan dess. Trots att ett antal ändringar förblir konfidentiella, offentliggjordes de gemensamma konsulära anvisningarna år 2000. När det gäller innehållet rör det sig i huvudsak en handbok som innehåller praktiska regler om hur viseringar för kortare vistelse skall utfärdas. De innehåller bestämmelser om granskning av ansökningar, förfarandena för beslutsfattande, och hur viseringsmärken skall fyllas i, osv.

2. INSAMLING AV BIOMETRISKA KÄNNETECKEN

2.1 Preliminär kommentar: Biometriska uppgifters specifika särdrag

Enligt förslaget om VIS ⁽¹⁾ som lades fram av kommissionen den 28 december 2004 skall medlemsstaterna införa fingeravtryck och fotografier som biometriska kännetecken i VIS av kontroll- och identifieringsskal. Det aktuella förslaget till Europaparlamentets och rådets förordning om ändring av de gemensamma konsulerä anvisningarna syftar till att tillhandahålla en rättslig grund för insamlingen av biometriska kännetecken.

Europeiska datatillsynsmannen avgav den 23 mars 2005 ett yttrande om VIS-förslaget ⁽²⁾. I detta yttrande betonade han betydelsen av att omgärda behandlingen av biometriska data med alla nödvändiga skyddsåtgärder med beaktande av deras specifika särdrag ⁽³⁾:

"Det är aldrig ett betydelselöst val att använda biometriska uppgifter i informationssystem, särskilt när systemet i fråga berör ett så stort antal människor. Biometri (...) ändrar oåterkalleligen förhållandet mellan kropp och identitet genom att göra människokroppens karakteristiska drag maskinläsbara och möjliga att använda vidare. Även om biometriska kännetecken inte kan ses av det mänskliga ögat kan de läsas och användas med lämpliga verktyg, för alltid, varhelst en person beger sig."

Enligt Europeiska datatillsynsmannen kräver biometriska uppgifters känsliga natur att införandet av skyldigheter för att använda dessa uppgifter endast bör ske efter en noggrann bedömning av riskerna med detta och bör följa ett förfarande som möjliggör full demokratisk kontroll. Dessa kommentarer ligger bakom Europeiska datatillsynsmannens granskning av det aktuella förslaget.

2.2. Bakgrunden till förslaget

Den bakgrund mot vilken detta förslag läggs fram gör det ännu mer känsligt. Den förordning som föreslås kan inte ses isolerad från utvecklingen av andra storskaliga IT-system och den allmänna tendensen till större interoperabilitet mellan olika informationssystem, något som uppmärksammas i kommissionens meddelande av den 24 november 2005 om förbättrad effektivitet, ökad interoperabilitet och förstärkta synergieffekter mellan de europeiska databaserna på området rättsliga och inrikes frågor ⁽⁴⁾.

Ett beslut som fattas i en viss situation och i ett visst syfte kommer troligen att påverka utvecklingen och användningen av andra system som byggs för andra ändamål. Bland annat biometriska uppgifter – som troligen samlats in för genomförande av viseringspolitiken – kan användas i olika sammanhang när de väl finns tillgängliga. Detta kan komma att gälla inte bara SIS utan med stor sannolikhet även Europol och Frontex (den europeiska gränsförvaltningsbyrån).

2.3. Skyldigheten att lämna fingeravtryck

I motiveringen till förslaget sägs följande: "Eftersom upptagandet av biometriska kännetecken nu kommer att bli en del av viseringsförfarandet, är det nödvändigt att ändra de gemensamma konsulerä anvisningarna för att skapa en rättslig grund för denna åtgärd."

Vad gäller de bestämmelser som rör huruvida vissa personer eller grupper av personer skall undantas eller ej från skyldigheten att lämna fingeravtryck, motsätter sig Europeiska datatillsynsmannen lagstiftarens val att ta in dessa bestämmelser i de gemensamma konsulerä anvisningarna snarare än i själva VIS-förordningen. Bestämmelserna har för det första en betydande inverkan på många personers privatliv och bör tas upp i den grundläggande lagstiftningen snarare än i anvisningar av övervägande teknisk karaktär. För att rättsreglerna skall framgå klart och tydligt är det för det andra att föredra att frågan tas upp i den text genom vilken själva informationssystemet inrättas.

⁽¹⁾ Förslag till Europaparlamentets och rådets förordning om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (KOM(2004) 835 slutlig) som lades fram av kommissionen den 28 december 2004.

⁽²⁾ Yttrande av den 23 mars 2005 om förslaget till Europaparlamentets och rådets förordning om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse, EUT C 181, 23.7.2005 s. 13.

⁽³⁾ "[Biometriska uppgifter] har en särprägel som är nästan total, dvs. varje individ har unik biometri. De ändras nästan aldrig under en människas liv, vilket gör dessa särdrag beständiga. Alla har samma fysiska beståndsdelar, vilket också ger biometrin en allmängiltig dimension.", ibid.

⁽⁴⁾ KOM(2005) 597 slutlig.

- a) För det första är skapandet av en rättslig grund för obligatoriskt upptagande av fingeravtryck och biometrisk kännetecken inte på något sätt bara en teknisk fråga, utan har stor inverkan på de berörda personernas integritet. Särskilt valet av minsta och/eller högsta ålder för upptagande av fingeravtryck är en politisk, inte bara teknisk, fråga. Europeiska datatillsynsmannen rekommenderar därför att dessa frågor, särskilt de som inte är av rent teknisk karaktär, tas upp i grundtexten (VIS-förslaget) och inte i en handbok med anvisningar som rör huvudsakligen de tekniska och praktiska aspekterna på viseringsförfarandet ⁽¹⁾.

Det är i detta sammanhang också lämpligt att erinra sig kraven i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (ECHR) och den rättspraxis som rör denna konvention. Enligt artikel 8.2 i ECHR får en offentlig myndighet inte ingripa i denna rätt till integritet annat än "med stöd av lag" och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till skyddet av viktiga intressen. I rättspraxis vid Europeiska domstolen för de mänskliga rättigheterna har dessa villkor medfört ytterligare krav på den rättsliga grunden för ingripandet (den måste ingå i tillgänglig lagstiftning och vara förutsägbar), på att varje åtgärd skall vara proportionell och på lämpliga garantier mot missbruk.

Bortsett från att det lagstiftningslappverk som beskrivs nedan inte reglerar dessa frågor på ett tydligt och tillgängligt sätt, kan man undra om själva de gemensamma konsulära anvisningarna ens kan betraktas som lagstiftning. Man kan ställa frågor rörande förfarandet för (eventuella) ändringar av denna text i framtiden. Det bör under alla omständigheter säkerställas att ett så viktigt beslut som detta inte kan ändras på annat sätt än genom ett förfarande med lämplig öppenhet och demokratiskt samråd.

- b) Den andra frågan rör rättsreglernas tydlighet. Av motiveringen till förslaget framgår inte klart varför det behövs skilda rättsliga grunder för insamlingen av biometriska uppgifter och för behandlingen av uppgifterna. I motiveringen sägs att "det här förslaget rör insamlingen av biometriska uppgifter, medan 'VIS-förslaget' omfattar översändande och utbyte av uppgifter." Från en dataskyddssynpunkt ingår emellertid i behandlingen av personuppgifter, insamlingen av dessa uppgifter. ⁽²⁾ Regleringen av olika operationer i en kedja av åtgärder i olika rättsakter kan vara till förfång för reglernas tydlighet. Detta är ett problem både för de (av detta förslag omfattade) registrerade personerna och för den demokratiska granskningen av systemet. Det blir i själva verket allt svårare att skaffa sig en fullständig bild på detta område, där i grund och botten samma behandling av uppgifterna regleras i olika delar av lagstiftningen.

2.4. Undantagen från upptagning av fingeravtryck

Detta problem illustreras på ett mycket bra sätt av frågan om vilka kategorier av personer som skall undantas från skyldigheten att lämna fingeravtryck, särskilt i fråga om små barn.

Hur tillåtligt det är att ta upp små barns fingeravtryck bör diskuteras mot bakgrund av syftet med själva VIS. Det måste med andra ord vara en proportionerlig åtgärd inom ramen för viseringspolitiken, och de därmed förbundna målen enligt VIS-förslaget, att föreskriva att vissa kategorier av personer är skyldiga att tillåta upptagande av biometriska kännetecken, eller att vissa personer undantas från denna skyldighet. Denna proportionalitet bör bedömas genom ett demokratiskt förfarande.

Den bör också bedömas mot bakgrund av hur fingeravtrycken kommer att användas enligt VIS-förslaget. Biometri kommer att användas antingen i kontrollsyfte eller för identifiering – ett biometriskt kännetecken kan bedömas vara tekniskt lämpligt för ett av dessa ändamål och inte för det andra. Bearbetning av fingeravtryck från barn under 14 år anses vanligen endast tillförlitlig för kontrolländamål. Detta bör påverka analysen av förslaget, men som framförts tidigare återfinns erforderliga led i VIS-förslaget (och omfattas ännu inte av något beslut).

Sammanfattningsvis rekommenderar Europeiska datatillsynsmannen med eftertryck att av tydlighets- och konsekvensskäl bör undantagen från upptagning av biometriska kännetecken enligt VIS-förordningen regleras strikt. Regleringen av insamlingen av biometriska kännetecken, i detta fall särskilt fingeravtryck, bör ses om ett till det rättsliga huvudinstrumentet underordnat led och därför behandlas i själva huvuddokumentet.

⁽¹⁾ Förhållandet att det rör sig om skilda rättsliga grunder – artikel 62.2 b.ii för de gemensamma konsulära anvisningarna och artikel 66 för VIS-förslaget – hindrar inte att lagstiftaren berör frågan i samma text.

⁽²⁾ Sidan 5 i motiveringen.

2.5 Ålder för viseringsökande

Det fastställs i förslaget att endast barn under sex år skall undantas från skyldigheten att lämna fingeravtryck. Detta föranleder många frågor (oavsett om detta kommer att omfattas av VIS-förslaget eller förslaget om de gemensamma konsulära anvisningarna).

För det första anser Europeiska datatillsynsmannen att ett generaliserat tagande av fingertryck på barn inte kan ses endast som en teknisk fråga utan kräver en seriös demokratisk debatt inom lämpliga institutioner. Ett sådant beslut bör inte grundas enbart på den tekniska genomförbarheten utan även, åtminstone, på de fördelar detta skulle innebära för genomförandet av VIS. Med undantag för ett mycket litet antal medlemsstater förefaller det dock som om det inte förekom någon offentlig debatt om denna fråga för närvarande, vilket är högst beklagligt.

Det måste även erinras om att VIS i princip har upprättats för att underlätta viseringsförfarandena för rese-
närer i god tro (majoriteten av resenärerna). Aspekter på lämplighet och ergonomi bör därför beaktas ⁽¹⁾. Användningen av biometriska kännetecken, oavsett om det är i förfarandet för viseringsansökningar eller vid gränskontrollerna, får inte innebära att viseringsförfarandet när det gäller barn blir för svårt att genomföra.

Det bör slutligen erinras om att alla system för biometriska kännetecken har tekniska brister. Den vetenskapliga litteraturen innehåller inte några avgörande bevis på att tagande av fingeravtryck på barn under 14 år möjliggör en tillförlitlig identifiering. De enda erfarenheterna hittills i fråga om större befolkningsgrupper är de som har gjorts med systemen Eurodac och US-Visit. Det är intressant att konstatera att man i båda systemen använder sig av fingeravtryck på barn som är 14 år eller äldre. Fingeravtryck på barn under denna ålder bör motiveras av undersökningar där deras tillförlitlighet och användbarhet inom ramen för en så stor-skalig databas som VIS, bevisas.

Under alla omständigheter vore det lämpligare att använda unga barns fingeravtryck för jämförelse av en grupp av uppgifter mot en annan snarare än för jämförelse av en grupp uppgifter mot flera andra. Detta bör uttryckligen anges.

Slutligen gäller de flesta av kommentarerna ovan inte bara barn utan också äldre. Tillförlitligheten och användbarheten av fingertryck avtar när människor åldras ⁽²⁾ och även aspekter på lämplighet och ergonomi är särskilt relevanta.

2.6 Fotografier

Samma sak kan sägas om fotografier för vilka det varken i detta förslag eller i VIS-förslaget har förutsetts någon åldersgräns. Man kan dock fråga sig om bilder av barn som är tagna innan de har uppnått sitt vuxna utseende verkligen är användbara i identifieringssyfte eller ens för kontroll.

Ansiktsgigenkänning av barn (såväl automatisk ansiktsgigenkänning i framtiden som "mänsklig" sådan) på grundval av referensbilder som är ett par år gamla bli troligtvis ett problem. Även om det har gjorts betydande framsteg för tekniken för ansiktsgigenkänning är det föga troligt att programvaran inom någon nära framtid skulle kunna kompensera effekterna av att ett barn vuxit på barnets ansikte. Det bör därför klargöras i VIS-förordningen att fotografier endast kan användas som ett stödande inslag för kontroll eller identifiering av personer så länge som tekniken för ansiktsgigenkänning inte är tillräckligt tillförlitlig, med beaktande av att detta troligen kommer att vara fallet för barn på längre sikt.

Allmänt sett rekommenderar Europeiska datatillsynsmannen när det gäller de båda biometriska kännetecknen att man noga överväger frågan om fördelarna (i kampen mot olaglig invandring och smuggling av barn) uppväger ovan angivna nackdelar.

2.7 Andra undantag

I förslaget anges det att "personer som det är fysiskt omöjligt att ta fingeravtryck på" skall undantas från kravet på fingeravtryck.

⁽¹⁾ Detta betonas i en undersökning på uppdrag av den nederländska regeringen, i J.E. DEN HARTOGH et al., *How do you measure a child? A study into the use of biometrics in children*, 2005, TNO.

⁽²⁾ Se t.ex. A. HICKLIN och R. KHANNA, *The Role of Data Quality in Biometric Systems*, MTS den 9 februari 2006.

Europeiska datatillsynsmannen har i sitt yttrande om VIS-förslaget redan understrukt att denna situation gäller för ett betydande antal personer: Upp till 5 % av befolkningen anses vara icke registrerbar. Med en databas på 20 000 000 registreringar per år innebär detta att det skulle kunna finnas upp till 1 000 000 fall per år där det finns svårigheter med registreringen. Detta är tveklöst något som man bör vara medveten om när förslaget analyseras. Europeiska datatillsynsmannen insisterade dessutom på behovet av effektiva säkerhetsprocedurer:

"Det bör finnas tillgång till säkerhetsprocedurer som utgör väsentliga skyddsåtgärder för införandet av biometri eftersom tekniken varken är tillgänglig för alla eller helt exakt. Sådana procedurer bör genomföras och användas för att respektera icke registrerbara personers värdighet och för att undvika att överföra problemet med systemets brister på dem"

I förslaget till förordning föreskrivs det att benämningen "ej tillämplig" skall föras in i VIS för dessa fall. Detta är mycket välkommet. Man kan dock befara att omöjligheten att registreras snarare skulle kunna leda till avslag på viseringsansökan. Om en mycket hög procentandel av omöjliga registreringar leder till avslag på viseringsansökningar, är detta inte godtagbart.

Det bör därför läggas till en bestämmelse i VIS-förordningen om att omöjlighet att registreras inte automatiskt får leda till ett negativt yttrande om utfärdandet av en visering. Det bör dessutom ägnas särskild uppmärksamhet i den rapportering som föreskrivs i VIS-förordningen för att behandla denna fråga: Man bör kontrollera om höga antal nekade viseringar är kopplade till omöjligheten att registreras.

3. Utläggning av viseringsansökningar på entreprenad

För att lätta bördan för varje medlemsstat (på grund av bland annat inköps- och underhållskostnader för utrustning) görs i förslaget flera samarbetsmekanismer möjliga:

- Samlokalisering: Personal från två eller flera medlemsstater behandlar de ansökningar (inklusive biometrisk kännetecken) som inlämnats till dem på en annan medlemsstats diplomatiska och konsulära beskickning och delar utrustningen med denna medlemsstat.
- Gemensamma ansökningskontor: Personal från två eller flera medlemsstaters diplomatiska beskickningar samlas i en byggnad och tar där emot de viseringsansökningar (inklusive biometrisk kännetecken) som är avsedda för dem.
- Slutligen anges det i förslaget att mottagandet av ansökningsformuläret och upptagningen av biometrisk kännetecken kan utföras av en extern tjänsteleverantör (detta alternativ förefaller vara sista utvägen för medlemsstater som inte kan använda en av de två andra alternativen, men detta är inte helt klart).

Förslaget går mycket långt för att säkerställa att endast tillförlitliga externa tjänsteleverantörer kan väljas och att dessa leverantörer måste kunna vidta alla nödvändiga åtgärder för att skydda uppgifter mot "mot förstöring genom olyckshändelse eller otillåtna handlingar eller förlust genom olyckshändelse samt mot ändringar, otillåten spridning av eller otillåten tillgång (...)" (artikel 1.B.2 i förslaget).

Denna bestämmelse är utformad med stor omsorg och noggrannhet för dataskydd, vilket Europeiska datatillsynsmannen välkomnar. Att bearbetningen av viseringsansökningar utförs av en extern tjänsteleverantör i ett tredje land har emellertid ett antal konsekvenser när det gäller skyddet av de (ibland mycket känsliga) uppgifter som samlas in för att utfärda viseringar.

Europeiska datatillsynsmannen betonar i synnerhet följande:

- Det kan visa sig mycket svårt, kanske till och med omöjligt att göra bakgrundskontroller av anställda på grund av det tredje landets lagstiftning eller praxis.
- På samma sätt kommer åläggandet av sanktioner mot anställda hos en extern leverantör för överträdelse av lagstiftningen till skydd för privatlivet inte nödvändigtvis att vara möjligt (även om avtalsrättsliga sanktioner kan tillämpas på den huvudsaklige entreprenören).
- Det privata företaget kan påverkas av politisk oro eller förändringar och inte vara i stånd att uppfylla sina skyldigheter när det gäller säkerheten i bearbetningen.
- Effektiv tillsyn kan vara svår att upprätta trots att det skulle vara ännu mer nödvändigt när det gäller externa partner.

Därför bör varje avtal med externa tjänsteleverantörer innehålla de nödvändiga skyddsåtgärderna för att säkerställa iakttagande av dataskydd, inbegripet extern revision, regelbundna stickprovskontroller, rapportering, mekanismer som säkerställer leverantörens ansvar i händelse av överträdelse av bestämmelser för att skydda privatlivet, inbegripet skyldigheten att kompensera enskilda som lidit skada till följd av en åtgärd från tjänsteleverantörens sida.

Utöver dessa frågor är det kanske ännu viktigare att vara medveten om att medlemsstaterna inte kommer att kunna garantera skyddet för den databehandling som lagts ut på entreprenad (eller den databehandling som utförs i gemensamma ansökningskontor om detta sker i en byggnad utanför diplomatiska beskickningslokaler) mot ett möjligt ingripande (t.ex. husrannsakan eller beslag) av sökandelandets offentliga myndigheter⁽¹⁾.

Externa tjänsteleverantörer kommer, trots alla andra avtalsbestämmelser, att omfattas av nationell lagstiftning i det tredje land där de har sitt säte. Händelser på senare tid avseende tillgång för myndigheter från ett tredje land till finansiella uppgifter som bearbetats av ett EU-företag visar att risken är långt från teoretisk. Vidare skulle detta kunna innebära en stor risk för berörda människor i en del tredjestater som gärna skulle vilja veta vilka av deras invånare som har ansökt om visering (för politisk kontroll av motståndare och oliktkäntande). Personal vid ett privat företag, i flertalet fall förmodligen lokalanställda, skulle inte vara i stånd att stå emot påtryckningar från regeringen eller brottsbekämpande myndigheter i de ansökarländer som begär uppgifter från dem.

Detta är en väsentlig svaghet i detta system jämfört med det fall då uppgifter bearbetas i en diplomatisk beskickningslokal. I det fallet skulle uppgifterna vara skyddade enligt Wienkonventionen av den 18 april 1961 om diplomatiska förbindelser. I artikel 22 i den konventionen föreskrivs det att

"Beskickningslokal skall vara okränkbar. Företrädare för den mottagande staten äger icke bereda sig tillträde dit utan beskickningschefens medgivande. (...) Beskickningslokal, dess inredning jämte övrig egendom som finnes där liksom beskickningens fortskaffningsmedel får ej bli föremål för husrannsakan, rekvisition, beslag eller exekutiva åtgärder".

Vidare, enligt artikel 4.1.b i direktiv 95/46/EG, skulle nationella bestämmelser om genomförande av direktivet också vara uttryckligen tillämpliga på denna bearbetning av personuppgifter, och stärka skyddet.

Det förefaller därför uppenbart att det enda effektiva sättet att skydda uppgifter som gäller viseringssökande och deras sponsorer (EU-medborgare eller företag) är att bevilja dem det skydd som ges enligt Wienkonventionen. Detta betyder att uppgifter bör bearbetas i lokaler med diplomatiskt skydd. Detta skulle inte hindra medlemsstaterna från att lägga ut bearbetningen av viseringsansökningar på entreprenad så länge den externa entreprenören kan utföra sin verksamhet i den diplomatiska beskickningens lokaler. Detta skulle också gälla för gemensamma ansökningskontor.

Därför skulle Europeiska datatillsyningsmannen starkt avråda ifrån alternativet att lägga ut behandlingen av viseringsansökningar på entreprenad till externa tjänsteleverantörer enligt artikel 15 i förslaget, ny punkt 1. B.1.b). I detta avseende är de godtagbara alternativen att

- lägga ut behandlingen av viseringsansökningar på entreprenad till ett privat företag så länge detta finns på en plats som skyddas genom diplomatisk status,
- lägga ut endast tillhandahållandet av information på entreprenad till en teletjänstcentral i enlighet med den föreslagna punkt 1.B.1.a).

4. SAMMANFATTNING

Europeiska datatillsyningsmannen välkomnar det faktum att detta förslag om ändring av de gemensamma konsulära anvisningarna kommer att antas genom medbeslutandeförfarandet, och därmed ökar den demokratiska granskningen på ett område där detta verkligen behövs.

⁽¹⁾ Detta problem föreligger resan när bearbetning av ansökningar görs av resebyråer. Det är emellertid ännu känsligare eftersom biometrisk uppgifter berörs, och eftersom anlitande av en resebyrå i princip inte är obligatoriskt.

I sakfrågan rekommenderar Europeiska datatillsyningsmannen följande:

- Undantagen från skyldigheten att tillhandahålla fingeravtryck bör behandlas i VIS-förordningen snarare än i de gemensamma konsulära anvisningarna, för att säkerställa klarhet och enhetlighet i detta system.
- Åldersgränserna för kraven på fingeravtryck och fotografier bör noga övervägas, med beaktande av genomförbarhetsaspekter, men överväganden bör också göras när det gäller etik, lämplighet och tillförlitlighet.
- Fotografier bör inte anses som en "fristående" identifiering utan endast som ett stödjande element.
- Att lägga ut behandlingen av viseringsansökningar på entreprenad till ett privat företag bör vara tillåtligt endast om det gäller en plats under diplomatiskt beskydd, och är baserat på avtalsklausuler som föreskriver effektiv tillsyn och entreprenörens ansvarighet.

Bryssel den 27 oktober 2006

Peter HUSTINX
Europeiska datatillsyningsmannen
