EUROPEISKA DATATILLSYNSMANNEN

Yttrande från Europeiska datatillsynsmannen om förslaget 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)

(2005/C 181/06)

EUROPEISKA DATATILLSYNSMANNEN HAR

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

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

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

med beaktande av 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, särskilt artikel 41, och

med beaktande av kommissionens begäran om yttrande i enlighet med artikel 28.2 i förordning (EG) nr 45/2001, mottagen den 25 januari 2005

ANTAGIT FÖLJANDE YTTRANDE:

1. INLEDNING

1.1 Inledande kommentarer

Inrättandet av Informationssystemet för viseringar (VIS) är en väsentlig del av EU:s gemensamma viseringspolitik och har varit föremål för flera sammanflätade instrument.

— I april 2003 framlades en genomförbarhetsstudie ([1]) om VIS som beställts av kommissionen.

— I september 2003 föreslog kommissionen en ändring ([2]) av en tidigare förordning om en enhetlig utformning av visumhandlingar. Huvudsyftet var att införa biometriska uppgifter (ansiktsbild och två fingeravtryck) i den nya utformningen av viseringar. Dessa biometriska uppgifter skulle lagras på ett mikrochip.

([1]) Visa Information System, slutrapport, beställd av kommissionen och utförd av Trasys, april 2003.
([2]) KOM (2003) 558 slutlig med 2003/0217 (CNS) och 2003/0218 (CNS).

— I juni 2004 inleddes genom ett rådsbeslut ([1]) uppbyggnaden av Informationssystemet för viseringar genom att en rättslig grund tillhandahölls för att införa detta i EU:s budget. I beslutet föreslogs en central databas med information om viseringsansökningar och ett kommittéförfarande föreskrevs för den tekniska utvecklingen av VIS.

I december 2004 antog kommissionen ett förslag till förordning om Informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse ([2]) (nedan kallat förslaget) som behandlas i detta yttrande. En utvidgad konsekvensanalys ([3]) (Extended impact assessment, nedan kallad den utvidgade konsekvensanalysen) bifogas förslaget.

Som nämns i motiveringen kommer det dock att behövas ytterligare rättsliga instrument som komplement till denna förordning, särskilt för att

— ändra de gemensamma konsulära anvisningar angående viseringar till diplomatiska beskickningar och karriärkonsulat för de avtalsslutande parterna i Schengenkonventionen (nedan kallade ”de gemensamma konsulära anvisningarna”) när det gäller införandet av biometriska uppgifter i förfarandena,

— utarbeta ett nytt system för utbyte av uppgifter med Irland och Förenade kungariket,

— utbyte av uppgifter om viseringar för längre vistelse.

Enligt beslut i rådet (rättsliga och inrikes frågor) den 5-6 juni 2003 och enligt beskrivningen i artikel 1.2 i det ovan nämnda rådsbeslutet från juni 2004 kommer VIS att baseras på en centraliserad struktur och bestå av en databas där filerna med viseringsansökningar kommer att lagras: Centrala informationssystemet för viseringar (CS-VIS), och ett nationellt gränssnitt (NI-VIS) i varje medlemsstat. Medlemsstaterna skall utse ([4]) en central nationell myndighet som är ansluten till det nationella gränssnittet och som ger de behöriga myndigheterna tillgång till CS-VIS.

1.2 **De viktigaste inslagen i förslaget med avseende på uppgiftsskydd**

Syftet med förslaget är att förbättra förvaltningen av den gemensamma viseringspolitiken genom att underlätta utbytet av uppgifter mellan medlemsstaterna genom inrättandet av en central databas. Enligt förordningen skulle biometriska uppgifter (foto och fingeravtryck) införas vid ansökningsförfarandet och lagras i den centrala databasen.

Biometriska uppgifter kan också användas i viseringsmärket, enligt i kommissionens förslag till ändringsförordning om en enhetlig utformning av visumhandlingar med införande av foto och fingeravtryck lagrade på ett mikrochip (avvaktar fortfarande rådsbeslut på grundval av resultatet av den pågående analysen).

I förslaget beskrivs i detalj de olika transaktioner som utförs i fråga om uppgifterna (införande, ändring radering och inhämtande) och de olika uppgifter som skall införas i VIS beroende på situationen när det gäller ansökan (godkännande, avslag, osv.).

I förslaget anges att uppgifter om varje ansökan skall lagras i fem år.

I förslaget förtecknas ett begränsat antal behöriga myndigheter utöver viseringsmyndigheterna som kommer att ha tillgång till VIS och deras rätt till tillgång fastställs:

— De behöriga myndigheter som utför kontroller av viseringar vid de yttre gränserna och inom medlemsstatens territorium.

— De behöriga invandringsmyndigheterna.

([1]) 2004/512/EG, EUT L 213, 15.6.2004, s. 5.
([2]) KOM (2004) 835 slutlig med 2004/0287 (COD).
([3]) Study for the Extended Impact Assesment of the Visa Information System, Slutrapport från EPEC, december 2004.
([4]) Artikel 24.2 i förslaget.

— De behöriga asylmyndigheterna.

I beskrivningen av driften av och ansvaret för VIS betonas i förslaget att kommissionen behandlar uppgifterna för medlemsstaternas räkning. Det redogörs för behovet att använda registren över uppgiftsbehandling för att säkerställa uppgifternas säkerhet och ansvaret för att säkerställa denna säkerhetsnivå redovisas i detalj.

Förslaget innehåller ett kapitel om uppgiftsskydd där rollerna för de nationella myndigheterna och Europeiska datatillsynsmannen (nedan kallad datatillsynsmannen) närmare anges.

Det tekniska genomförandet av VIS och valet av teknik skulle enligt förslaget ombesörjas av en kommitté enligt artikel 5.1 i förordning (EG) nr 2424/2001 om utvecklingen av andra generationen av Schengens informationssystem (SIS II).

En utvidgad konsekvensanalys av VIS som beställts av kommissionen och genomförts av EPEC bifogas förslaget. Där dras slutsatsen att alternativet VIS tillsammans med användning av biometri är den bästa tillgängliga lösningen för att förbättra den gemensamma viseringspolitiken.

2. **TILLÄMPLIG RAM**

Förslaget kommer att ha stor påverkan på den personliga integriteten och andra grundläggande rättigheter för enskilda människor. Det skall därför kontrolleras med avseende på principerna om personuppgiftsskydd. De främsta referenspunkterna för vår granskning är följande:

— Respekten för privatlivet har varit garanterad i Europa alltsedan Europarådet 1950 antog konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (nedan kallad ECHR). I artikel 8 i ECHR fastställs ”rätt till skydd för privat- och familjeliv”.

  Enligt artikel 8.2 får en offentlig myndighet inte ingripa i denna rättighet annat än ”med stöd av lag” och ”om det i ett demokratiskt samhälle är nödvändigt” för att skydda väsentliga intressen. I rättspraxis vid Europeiska domstolen för de mänskliga rättigheterna har dessa villkor föranlett kompletterande krav på kvaliteten på den rättsliga grunden för ingripande, åtgärdernas proportionalitet och behovet av lämpliga skyddsåtgärder mot missbruk.

  Grundläggande principer för skydd av enskilda vid behandling av personuppgifter har utvecklats i konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter, som utarbetats av Europarådet och antogs 1981.

— Rätten till respekt för privatlivet och skydd av personuppgifter har på senare tid fastställts i artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna, vilken har införlivats i del II i den nya EU-konstitutionen.

  Enligt artikel 52 i stadgan erkänns att dessa rättigheter kan begränsas under förutsättning att likvärdiga villkor som enligt artikel 8 i ECHR är uppfyllda. Dessa villkor måste beaktas vid varje bedömning av ett förslag om eventuellt ingripande.

För närvarande fastställs de grundläggande reglerna för personuppgiftsskydd i EU-lagstiftningen i följande rättsakter:

— 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 (EGT L 281, s. 31). Direktivet kommer nedan att kallas direktiv 95/46/EG. I direktivet anges närmare principer mot vilka förslaget kommer att stämmas av med avseende på i vilken utsträckning det bör tillämpas på medlemsstaterna. Detta är högst relevant eftersom förslaget kommer att gälla tillsammans med den nationella lagstiftning genom vilken direktivet får verkan. Effektiviteten av de föreslagna bestämmelserna och skyddsåtgärderna kommer därför att vara beroende av hur effektiv denna kombination är i varje enskilt fall.

— 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 (EGT L 8, s. 1). Denna förordning kommer nedan att kallas förordning nr 45/2001. I denna föreskrivs liknande principer som i direktiv 95/46/EG, och den är relevant i detta sammanhang i den mån som förslaget skall gälla kommissionens verksamhet tillsammans med bestämmelserna i förordningen. Denna kombination förtjänar därför också en viss uppmärksamhet.

Direktiv 95/46/EG och förordning nr 45/2001 måste jämföras med andra instrument. Med andra ord måste direktivet och förordningen, i den mån de avser behandling av personuppgifter som kan inskränka de grundläggande friheterna, särskilt rätten till respekt för privatlivet, tolkas mot bakgrund av de grundläggande rättigheterna. Detta följer också av domstolens rättspraxis ([1]).

— Slutligen vill datatillsynsmannen i sin analys också ta med yttrande nr 7/2004 av den 11 augusti 2004 av EU:s arbetsgrupp för personuppgiftsskydd (den s.k. Artikel 29-kommittén) ([2]) om införande av biometriska kännetecken i uppehållstillstånd och viseringar med hänsyn till inrättandet av Informationssystemet för viseringar (VIS). I yttrandet uttryckte arbetsgruppen betänkligheter beträffande flera inslag i förslaget. Datatillsynsmannen avser att kontrollera om och hur dessa betänkligheter har beaktats i förslaget.

3. ANALYS AV FÖRSLAGET

3.1 Allmänt

Datatillsynsmannen erkänner att vidareutvecklingen av den gemensamma viseringspolitiken kräver ett effektivt utbyte av relevanta uppgifter. VIS är en av de mekanismer som kan sörja för ett smidigt informationsflöde. Ett sådant nytt instrument bör dock begränsas till insamling och utbyte av uppgifter i den mån insamlingen eller utbytet är nödvändigt för att utarbeta en gemensam viseringspolitik och står i proportion till målet.

Inrättandet av VIS kan ha positiva konsekvenser för andra berättigade samhällsintressen, men detta ändrar inte syftet med VIS. Systemets begränsade syfte spelar stor roll vid fastställandet av dess legitima innehåll och användning och därför också vid beviljande av tillgång till VIS (eller delar av uppgifterna i detta) för medlemsstaternas myndigheter för berättigade samhällsintressen.

Dessutom införs genom förslaget användning av biometri i VIS. Datatillsynsmannen inser fördelarna med användning av biometri, men betonar de omfattande konsekvenser som användningen av sådana uppgifter medför och föreslår att strikta skyddsåtgärder införs för användningen av biometriska uppgifter.

Yttrandet bör läsas mot bakgrund av dessa huvudsakliga synpunkter. Det bör påpekas att detta yttrande bör nämnas i förordningens ingress före skälen (”med beaktande av … yttrande …”).

([1]) Det är i detta sammanhang lämpligt att hänvisa till domstolens dom av den 20 maj 2003 i förenade målen C-465/00, C-138/01 och C-139/01, Österreichischer Rundfunk m.fl., REG 2003, s. I-4989. Domstolen behandlade en österrikisk lag om överföring och påföljande offentliggörande av löneuppgifter för offentligt anställda till den österrikiska revisionsrätten. I domen fastställer domstolen ett antal kriterier som bygger på artikel 8 i Europakonventionen om skydd för de mänskliga rättigheterna vilka bör användas vid tillämpning av direktiv 95/46/EG, eftersom vissa begränsningar av rätten till respekt för privatlivet möjliggörs genom detta direktiv.

([2]) Detta är en oberoende rådgivande grupp sammansatt av företrädare för medlemsstaternas dataskyddsmyndigheter, datatillsynsmannen och kommissionen, som inrättades genom direktiv 95/46/EG.

3.2 **Syfte**

Syftet med VIS har mycket stor betydelse, både mot bakgrund av artikel 8 i ECHR och av den allmänna ramen för uppgiftsskydd. Enligt artikel 6 i direktiv 95/46/EG skall personuppgifter ”samlas in för särskilda, uttryckligt angivna och berättigade ändamål; senare behandling får inte ske på ett sätt som är oförenligt med dessa ändamål”. Endast en tydlig definition av syftet kommer att möjliggöra en korrekt bedömning av om behandlingen av personuppgifter är proportionerlig och adekvat. Detta är av avgörande betydelse på grund av uppgifternas art (inklusive biometri) och omfattningen av den planerade behandlingen.

Syftet med VIS anges klart i artikel 1.2 i förslaget:

> ”VIS skall förbättra förvaltningen av den gemensamma viseringspolitiken, det konsulära samarbetet och samrådet mellan centrala konsulära myndigheter genom att underlätta utbytet av uppgifter mellan medlemsstaterna om viseringsansökningar och de beslut som fattas i anslutning till dessa”.

Alla delar av VIS måste därför vara nödvändiga och proportionerliga instrument för att uppnå detta politiska mål till förmån för den gemensamma viseringspolitiken.

I artikel 1.2 i förslaget förtecknas också ytterligare fördelar med förbättringen av viseringspolitiken, t.ex. att

a) förebygga hot mot den inre säkerheten,

b) underlätta kampen mot bedrägerier,

c) underlätta kontrollen vid kontrollställena vid de yttre gränserna.

Datatillsynsmannen betraktar dessa inslag som exempel på positiva konsekvenser av inrättandet av VIS och förbättringen av den gemensamma viseringspolitiken, men inte som syften i sig.

Detta leder till två väsentliga konsekvenser i detta skede:

— Datatillsynsmannen är medveten om att de brottsbekämpande myndigheterna är intresserade av att beviljas tillgång till VIS; rådet antog slutsatser i denna riktning den 7 mars 2005. Eftersom syftet med VIS är förbättring av den gemensamma viseringspolitiken bör det noteras att rutinmässig tillgång för brottsbekämpande myndigheter inte skulle vara förenligt med detta syfte. Samtidigt som sådan tillgång under vissa omständigheter och med förbehåll för lämpliga skyddsåtgärder kan beviljas *ad hoc* i enlighet med artikel 13 i direktiv 95/46/EG kan en systematisk tillgång inte medges.

  Mer allmänt är en bedömning av proportionaliteten och nödvändigheten avgörande om beslut i framtiden fattas om huruvida vissa andra myndigheter skall beviljas tillgång till VIS. De uppdrag för vilka tillgång beviljas måste vara förenliga med syftet med VIS.

— Det uttryckliga omnämnandet av att ”förebygga hot mot den inre säkerheten i någon av medlemsstaterna” i a) är beklagligt. De främsta fördelarna med VIS kommer att vara förebyggandet av bedrägerier och visa shopping (kampen mot bedrägerier är också huvudskälet för att införa biometri i systemet). ([1]) Förebyggandet av hot mot säkerheten bör därför betraktas som en sekundär men ändå mycket välkommen fördel.

  Datatillsynsmannen rekommenderar att skillnaden mellan syfte och fördelar förtydligas i artikel 1.2, exempelvis på följande sätt:

  > ”VIS har till syfte att förbättra förvaltningen av den gemensamma viseringspolitiken, det konsulära samarbetet och samrådet mellan centrala konsulära myndigheter genom att underlätta utbytet av uppgifter mellan medlemsstaterna om viseringsansökningar och de beslut som fattas i anslutning till dessa. I samband härmed skall det också bidra …”

([1]) I den utvidgade konsekvensanalysen anges detta mycket tydligt (punkt 2.7 på s. 6): *”ineffektiviteten vid bekämpandet av visa shopping, bedrägerier och vid kontroller orsakar också ineffektivitet när det gäller medlemsstaternas inre säkerhet”*. Detta innebär att hoten mot säkerheten delvis beror på en ineffektiv viseringspolitik. Det första som bör göras härvidlag är att förbättra viseringspolitiken, främst genom att bekämpa bedrägerier och genomföra bättre kontroller. Förbättringen av säkerheten kommer att följa av förbättringen av viseringspolitiken.

I detta sammanhang kan det också noteras att de ”riktlinjer för införande av ett gemensamt system för utbyte av viseringsuppgifter” som antogs av RIF-rådet den 13 juni 2002 [1] placerade förebyggandet av hot mot den inre säkerheten sist. Detta skulle också vara möjligt och mycket mer förenligt med syftet med VIS.

3.3 **Uppgifternas kvalitet**

Enligt artikel 6 i direktiv 95/46/EG gäller för personuppgifter att de skall ”vara adekvata och relevanta och inte får omfatta mer än vad som är nödvändigt med hänsyn till de ändamål för vilka de har samlats in och för vilka de senare behandlas”. Detta gäller proportionaliteten i själva VIS men även de uppgifter som skall samlas in och lagras i VIS och deras framtida användning samt de ytterligare skyddsåtgärder som gäller i samband härmed. Dessa faktorer är likaledes väsentliga för utvärderingen av förslaget mot bakgrund av artikel 8 i ECHR.

Inrättandet av VIS innebär utan tvivel ett viktigt ingrepp i utövandet av rätten till respekt för privatlivet med tanke på dess omfattning och den kategori av personuppgifter som behandlas. Därför begärde arbetsgruppen för skydd av enskilda vid behandlingen av personuppgifter i sitt yttrande nr 7/2004 att få reda på vilka undersökningar av omfattningen av och allvaret hos dessa företeelser som visade på tvingande skäl med hänsyn till allmän säkerhet eller ordning och som skulle motivera ett sådant tillvägagångssätt.

Datatillsynsmannen har noggrant noterat de belägg som framfördes i den utvidgade konsekvensanalysen. Även om dessa inte är helt avgörande tycks det finnas tillräckliga skäl att motivera inrättandet av VIS i syfte att förbättra den gemensamma viseringspolitiken.

I detta sammanhang torde det ligga inom lagstiftarens utrymme för bedömning att besluta om inrättandet av VIS som ett instrument för att förbättra villkoren för medlemsstaternas utfärdande av viseringar. Ett sådant system kan i sig väl passa in och stärka det successiva upprättandet av ett område med frihet, säkerhet och rättvisa i enlighet med EG-fördraget.

Inrättandet och användningen av VIS kan dock aldrig få till följd att en hög skyddsnivå för personuppgifter inte längre kan garanteras på detta område. Det ingår i den rådgivande uppgiften för datatillsynsmannen att undersöka i vilken utsträckning VIS kommer att påverka den befintliga uppgiftsskyddsnivån för de registrerade som berörs.

Mot denna bakgrund kommer datatillsynsmannen i sitt yttrande att koncentrera sig på följande frågor:

— Uppgifternas proportionalitet och lämplighet och användningen av dessa (t.ex. kategorier av uppgifter, tillgång till uppgifter för varje berörd myndighet och lagringstid).

— Driften av systemet (t.ex. ansvar och säkerhet).

— De registrerades rättigheter (t.ex. information, möjlighet att korrigera eller radera felaktiga eller icke relevanta uppgifter).

— Övervakning och kontroll av systemet.

Frånsett följande punkter föranleder förslaget inga viktiga kommentarer när det gäller vilka kategorier av uppgifter som skall införas i VIS och deras användning. De aktuella bestämmelserna har formulerats omsorgsfullt och förefaller på det hela taget konsekventa och adekvata.

---

[1] Rådets rambeslut av den 13 juni 2002 om bekämpande av terrorism (2002/475/RIF), EGT L 164, 22.6.2002, s. 3.

3.4 **Biometri**

3.4.1 *Konsekvens av användning av biometriska uppgifter*

Det är aldrig ett betydelselöst val att använda biometriska uppgifter i informationssystem, särskilt när systemet i fråga berör ett så stort antal människor. Biometri är mer än bara en ny informationsteknik. Den 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, varthelst en person beger sig.

Hur användbara biometriska uppgifter än kan vara för vissa ändamål kommer en allmänt spridd användning av dessa att ha betydande samhällskonsekvenser och bör vara föremål för en bred och öppen debatt. Datatillsynsmannen måste konstatera att denna debatt faktiskt inte har ägt rum innan förslaget utarbetades. Detta understryker i ännu högre grad behovet av strikta skyddsåtgärder för användning av biometriska uppgifter och ingående reflexion och debatt under lagstiftningsprocessens gång.

3.4.2 *De biometriska uppgifternas särskilda karaktär*

Som den s.k. Artikel 29-kommittén redan har betonat i flera yttranden ([1]) måste införandet och behandlingen av biometriska uppgifter i identitetshandlingar stödjas av särskilt konsekventa och betydande skyddsåtgärder. Biometriska uppgifter är på grund av vissa särdrag mycket känsliga.

Det är sant att det är nästan omöjligt för den berörda personen att förlora biometriska uppgifter, till skillnad från ett lösenord eller en nyckel. De har en *särprägel som är nästan total*, d.v.s. 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.

Det är emellertid nästan omöjligt att återkalla biometriska uppgifter: ett finger eller ansikte är svårt att förändra. Detta positiva särdrag innebär ur många perspektiv en stor nackdel i händelse av *identitetsstöld*: lagringen av fingeravtryck och fotografier i en databas kopplad till en stulen identitet kan leda till stora och kvarstående problem för den verklige innehavaren av denna identitet. Dessutom är biometriska uppgifter genom sin karaktär *inte hemliga* och kan till och med *lämna spår* (fingeravtryck, DNA) som gör att uppgifterna kan samlas in *utan att innehavaren är medveten* om detta.

På grund av dessa risker som ligger i biometrins natur måste betydande skyddsåtgärder genomföras (särskilt när det gäller respekten för principen om begränsning av syftet, begränsning av tillgången och säkerhetsbestämmelser).

3.4.3 *Tekniska brister hos fingeravtryck*

De främsta fördelarna med biometri enligt ovan (uppgifternas allmängiltighet, särprägel, beständighet, användbarhet, osv.) är aldrig absoluta. Detta har direkt inverkan på effektiviteten av de biometriska registrerings- och kontrollförfaranden som planeras i förordningen.

Upp till 5 % av alla människor bedöms ([2]) inte kunna registreras (eftersom de inte har några läsbara fingeravtryck eller inga fingeravtryck alls). I den utvidgade konsekvensanalys som bifogas förslaget räknar man med ca 20 miljoner viseringssökande 2007, vilket innebär att upp till 1 miljon personer inte kommer att kunna följa den ”normala” registreringsprocessen, med uppenbara konsekvenser för ansökan om visering och vid gränskontrollen.

([1]) Yttrande 7/2004 om införande av biometriska kännetecken i uppehållstillstånd och viseringar med beaktande av införandet av informationssystemet för viseringar (VIS) (Markt/11487/04/EN - WP 96) och arbetsdokument om biometri (MARKT/10595/03/EN - WP 80).

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

Biometrisk identifiering är också per definition en statistisk process. En felfrekvens på 0,5-1 % är normal ([1]) vilket innebär att systemet för kontroll vid de yttre gränserna kommer att ha en frekvens av felaktiga avvisningar på mellan 0,5 och 1 %. Denna frekvens stäms av genom en tröskel grundad på de behöriga myndigheternas riskpolicy (den motsvarar en balans som fastställs mellan antalet personer som felaktigt avvisas och personer som felaktigt godkänns). Det är därför en överdrift att anse att denna teknik kommer att ge en ”exakt identifiering” av den registrerade, vilket uppges i skäl 9 i förslaget till förordning.

Enligt en nyligen genomförd framtidsstudie ([2]) som beställts av Europaparlamentets LIBE-utskott bör det 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. ([3])

Datatillsynsmannen rekommenderar därför att säkerhetsprocedurer utarbetas och införs i förslaget. Dessa procedurer bör varken sänka viseringspolitikens säkerhetsnivå eller stigmatisera enskilda personer med oläsbara fingeravtryck.

3.5 **Särskilda kategorier av uppgifter**

Några kategorier av uppgifter (utöver biometriska uppgifter) kräver särskild eftertanke: uppgifter om orsaker till avslag på ansökan om visering (3.4.1) och uppgifter om andra medlemmar i en grupp (3.4.2).

3.5.1 *Grunder för avslag på ansökan om visering*

I artikel 10.2 i förslaget föreskrivs behandling av uppgifter om grunderna för avslag när beslut har fattats om att avslå ansökan om visering. Dessa grunder för avslag är helt standardiserade.

— De båda första grunderna i led a och b är av tämligen administrativ art: Den sökande har inte kunnat uppvisa en giltig resehandling, eller giltiga handlingar som styrker syftet med och förutsättningarna för den planerade vistelsen.

— I led c nämns att ”den sökande finns upptagen på spärrlista” vilket inbegriper användning av SIS-databasen.

— Slutligen anges i led d som ett skäl att avslå ansökan om visering att den sökande ”utgör ett hot mot någon av medlemsstaternas allmänna ordning, inre säkerhet, folkhälsa eller internationella förbindelser”.

([1])

Biometri	Ansikte	Finger	Iris
FTE % Failure To Enrol	n/a	4	7
FNMR % rejection rates	4	2,5	6
FMR1 % verification match error rate	10	< 0,01	< 0,001
FMR2 % identification error rates for dB size> 1m	40	0,1	N/A
FMR3 % screening match error rate for dB sizes = 500	12	< 1	N/A

Jain, A. K. m.fl., *Biometrics: A grand challenge*, Proceedings of International Conference on Pattern Recognition, Cambridge, UK, augusti 2004.

([2]) *Biometrics at the frontiers: assessing the impact on Society*, februari 2005, Institutet för teknologiska framtidsstudier, GD gemensamma forskningscentret, kommissionen.

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

Alla grunder för avslag måste tillämpas med stor försiktighet på grund av de följder som de medför för den enskilde. Dessutom kommer vissa av dem - led c och d - att leda till behandling av ”känsliga uppgifter” i den mening som avses i artikel 8 i direktiv 95/46/EG.

Datatillsynsmannen skulle särskilt vilja uppmärksamma villkoret ”folkhälsa”, vilket förefaller vagt och leder till behandling av mycket känsliga uppgifter. Enligt kommentaren till artiklarna i förslagets bilaga är hänvisningen till hot mot folkhälsan grundad på förslaget till rådets förordning om en gemenskapskodex om gränspassage för personer (KOM (2004) 391 slutlig).

Datatillsynsmannen är medveten om att kriteriet ”folkhälsa” används allmänt i gemenskapslagstiftningen rörande den fria rörligheten för personer och att det tillämpas mycket strikt, vilket framgår av Europaparlamentets och rådets direktiv 2004/38/EG av den 29 april 2004 om unionsmedborgares och deras familjemedlemmars rätt att fritt röra sig och uppehålla sig inom medlemsstaternas territorier. I artikel 29 i direktivet fastställs villkoren för beaktande av folkhälsan: ”De enda sjukdomar som kan motivera åtgärder som begränsar den fria rörligheten skall vara sjukdomar som kan vara epidemiska enligt Världshälsoorganisationens gällande bestämmelser samt andra smittsamma infektions- eller parasitsjukdomar om de i den mottagande medlemsstaten omfattas av skyddsbestämmelser som gäller för de egna medborgarna”.

— Det bör dock noteras att det förslag som det hänvisades till tidigare hittills är just ett förslag, och att förutsättningen för att innefatta villkoret att inte utgöra ett hot mot folkhälsan i VIS-förordningen är att gemenskapskodexen antagits.

— Om gemenskapskodexen antas bör denna grund för avslag dessutom uppfattas restriktivt. Förslaget till gemenskapskodex är för övrigt i sin tur grundat på det ovan nämnda direktiv 2004/38/EG.

Datatillsynsmannen rekommenderar därför att en hänvisning till artikel 29 i direktiv 2004/38/EG införs i förslaget för att säkerställa att ”hot mot folkhälsan” uppfattas mot bakgrund av denna bestämmelse. Med tanke på uppgifternas känslighet bör de i alla händelser endast behandlas om det verkligen föreligger ett hot mot folkhälsan som är tillräckligt allvarligt.

3.5.2 *Uppgifter om andra gruppmedlemmar*

I artikel 2.7 definieras *gruppmedlem* som ”andra sökande som en sökande reser tillsammans med, inklusive medföljande make/maka och barn till den sökande”. I kommentaren till artiklarna sägs att definitionerna i artikel 2 i förslaget hänvisar till fördraget eller Schengenregelverket om viseringspolitik, förutom några termer, däribland *gruppmedlem*, som definieras särskilt för denna förordning. Det kan därför antas att denna definition inte avser definitionen av *gruppviseringar* enligt artikel 2.1.4 i de gemensamma konsulära anvisningarna. I kommentaren till artiklarna hänvisas till sökande som reser i en grupp tillsammans med andra sökande, t.ex. inom ramen för ett ADS-avtal (ADS - Approved Destination Status, status som godkänt resmål) eller tillsammans med familjemedlemmar.

Datatillsynsmannen betonar att det bör finnas en exakt och heltäckande definition av *gruppmedlemmar* i förordningen. Enligt datatillsynsmannen är definitionen alltför vag i det nuvarande förslaget, eftersom det saknas en klar hänvisning till fördraget eller Schengenregelverket. Med nuvarande formulering kan *gruppmedlemmar* inbegripa kolleger, andra resenärer från samma resebyrå som deltar i en organiserad resa, osv. Följderna är betydande:

enligt artikel 5 i utkastet till förordning skall en ansökan för en sökande länkas till övriga gruppmedlemmars ansökningar.

3.6 **Lagringstid för uppgifterna**

I artikel 20 i utkastet till förordning föreskrivs fem års lagringstid för varje ansökan. Det är en policy som har valts så att gemenskapslagstiftaren kan ge en rimlig tidsfrist.

Det finns ingenting - särskilt inte mot bakgrund av de skäl som nämns i kommentaren till artiklarna - som tyder på att valet av policy i förslaget är orimligt eller skulle få oacceptabla följder, förutsatt att alla korrigeringsmekanismer som är lämpliga fungerar. Detta betyder att det måste säkerställas att uppgifter korrigeras eller raderas när de inte längre är korrekta, och detta särskilt när en person har erhållit medborgarskap i en medlemsstat eller har erhållit en status som inte kräver att han finns upptagen i systemet.

Medan uppgifterna fortfarande finns kvar i systemet får de dessutom under inga förhållanden inverka menligt på ett nytt beslut. Vissa grunder för avslag (den sökande finns upptagen på spärrlista, i synnerhet utgör hot mot folkhälsan) har en begränsad giltighetstid. Även om de vid en viss tidpunkt har utgjort giltiga grunder för avslag bör detta faktum inte påverka ett nytt beslut. En helt ny bedömning av situationen måste göras för varje ny viseringsansökan och detta bör uttryckas klart i förordningen där så är lämpligt.

3.7 **Tillgång till och användning av uppgifter**

3.7.1 *Inledande synpunkter*

Som en inledande synpunkt erkänner datatillsynsmannen att regelsystemet för tillgång till och användning av VIS-uppgifter uppenbarligen ägnats stor omsorg. Varje myndighet har tillgång till olika uppgifter för olika syften. Detta är ett lämpligt tillvägagångssätt som datatillsynsmannen gärna vill uppmuntra. Syftet med följande anmärkningar är att tillämpa denna metod fullt ut.

3.7.2 *Kontroller av viseringar vid yttre gränser och inom territoriet*

När det gäller kontroller av viseringar vid yttre gränser nämns i artikel 16 i förslaget till förordning följande båda syften klart:

— Kontroll av en persons identitet, vilket i enlighet med den givna definitionen innebär en jämförelse av en grupp av uppgifter mot en annan.

— Kontroll av viseringens äkthet. Enligt ICAO:s normer skulle ett system med öppet/hemlig nyckel (PKI) kunna användas på viseringens mikrochip för denna äkthetskontroll.

Dessa båda syften kan uppnås på ett korrekt sätt om endast de behöriga myndigheterna får tillgång till det skyddade mikrochipet för att kontrollera viseringar. Tillgång till VIS centrala databas skulle därför vara orimlig i detta särskilda fall. Detta sistnämnda alternativ skulle involvera fler myndigheter som är anslutna till VIS, vilket skulle kunna öka risken för missbruk. Det skulle även kunna bli ett dyrare alternativ eftersom den säkra och kontrollerade tillgången till VIS skulle öka avsevärt och därmed även behovet av särskild utbildning i samband med detta.

Det råder dessutom tveksamhet om huruvida den tillgång till uppgifter som avses i artikel 16.2 är lämplig. I artikel 16.2 a fastställs det visserligen att om en första sökning visar att det finns uppgifter om den sökande i VIS (vilket i princip borde vara fallet), skall den behöriga myndigheten ges tillgång till andra uppgifter, dock endast för att kunna kontrollera en persons identitet. Dessa uppgifter avser all information som rör ansökan, t. ex fotografier, fingeravtryck, liksom även om eventuella tidigare utfärdade, ogiltigförklarade, återkallade eller förlängda viseringar.

Om identitetskontrollen har lyckats, är det mycket oklart varför de övriga uppgifterna fortfarande behövs. De bör bara lämnas ut, under restriktiva villkor, om kontrollen har misslyckats. I detta fall skulle de uppgifter som avses i artikel 16.2 på ett lämpligt sätt bidra till en reservmetod för att bidra till att fastställa personens identitet. All personal vid kontrollställena bör inte ha tillgång till uppgifterna, utan endast de tjänstemän som har hand om komplicerade fall.

Slutligen bör definitionen av de myndigheter som har tillgång till uppgifterna vara mer exakt. I synnerhet är det oklart vilka ”De behöriga myndigheter som ansvarar för kontrollen […] inom medlemsstatens territorium …” är. Datatillsynsmannen antar att detta avser de behöriga myndigheter som ansvarar för kontrollen *av viseringar*, och artikel 16 bör ändras i detta avseende.

3.7.3 *Användning av uppgifter för identifiering och återsändande av olagliga invandrare och för asylförfaranden*

I de fall som beskrivs i artiklarna 17-19 (återsändande av olagliga invandrare och asylförfarande) används VIS för identifiering. Bland de uppgifter som kan användas för identifiering finns fotografier. I det rådande läget på området teknik rörande automatiserad ansiktsigenkänning för detta slag av storskaliga IT-system kan fotografier dock inte användas för identifiering (databassökning mot flera grupper av uppgifter), eftersom de inte ger tillförlitliga resultat. De skall därför inte anses lämpliga för identifieringssyften.

Datatillsynsmannen förordar därför bestämt att ”fotografier” tas bort från första delen av dessa artiklar men behålls i andra delen (fotografier kan användas som verktyg för att kontrollera en persons identitet men inte för identifiering i en storskalig databas).

Ett annat alternativ vore att ändra artikel 36 på sådant sätt att funktionerna för att behandla fotografier för identifieringssyfte inte genomförs förrän denna teknik kan anses tillförlitlig (eventuellt efter utlåtande från tekniska kommittén).

3.7.4 *Offentliggörande av de myndigheter som har tillgång*

I artikel 4 i utkastet till förordning föreskrivs det att en förteckning över de behöriga myndigheter som i varje medlemsstat utsetts att ha tillgång till VIS skall offentliggöras i *Europeiska unionens officiella tidning*. Detta offentliggörande skall göras regelbundet (årligen) för att informera om förändringar av den nationella situationen. Datatillsynsmannen framhåller att offenliggörandet är viktigt som ett oumbärligt kontrollredskap både på europeisk och nationell eller lokal nivå.

3.8 **Ansvar**

Det erinras här om att VIS kommer att bygga på en centraliserad struktur med en central databas där all information om viseringar kommer att lagras och på nationella gränssnitt i medlemsstaterna som ger deras behöriga myndigheter tillgång till det centrala systemet. I enlighet med skäl 14 och 15 i utkastet till förordning kommer direktiv 95/46/EG att tillämpas för medlemsstaternas behandling av personuppgifter vid tillämpning av förordningen och förordning 45/2001 kommer att tillämpas för kommissionens verksamhet när det gäller skyddet av personuppgifter. Enligt skälen i ingressen är förslagets syfte att klargöra vissa punkter, bland annat rörande ansvaret för användningen av uppgifter och kontrollen av uppgiftsskyddet.

Dessa punkter verkar röra vissa avgörande frågor utan vilka systemet med skyddsåtgärder i direktiv 95/46/EG och förordning 45/2001 inte skulle gälla eller inte överensstämma till fullo med förslaget. Den nationella lagstiftningens tillämplighet enligt direktivet förutsätter vanligen en registeransvarig som är etablerad i den medlemsstaten (artikel 4) medan förordningens tillämplighet beror på gemenskapsinstitutioners eller gemenskapsorgans behandling av personuppgifter, om denna behandling genomförs för att utföra uppgifter som helt eller delvis omfattas av gemenskapsrätten (artikel 3).

Enligt artikel 23.2 i utkastet till förordning skall ”Uppgifterna […] behandlas av VIS för medlemsstaternas räkning”. Enligt artikel 23.3 skall varje medlemsstat utse den myndighet som skall fungera som registeransvarig i den mening som avses i artikel 2 d i direktiv 95/46/EG. Detta verkar innebära att kommissionen, enligt direktivets system, skulle fungera som registerförare. Detta bekräftas i förklaringen till artiklarna ([1]).

Denna lydelse bidrar till att förminska kommissionens mycket viktiga och faktiskt avgörande roll, både under systemets utvecklingsskede och under dess normala drift. Det är svårt att direkt koppla kommissionens roll till funktionen som registeransvarig eller registerförare; antingen är den en registerförare med ovanliga befogenheter (bland annat vid utformnigen av systemet) eller en registeransvarig med begränsade uppgifter (eftersom uppgifterna förs in och används av medlemsstaterna). Kommissionen har vad i praktiken måste anses vara en roll i sitt eget slag ([2]) i VIS.

Denna viktiga roll bör erkännas genom en övergripande beskrivning av kommissionens uppgifter och inte genom en lydelse som inte helt motsvarar verkligheten därför att den är alltför restriktiv, inte ändrar något i VIS funktion och endast leder till förvirring. Detta är även viktigt med tanke på en enhetlig och effektiv övervakning av VIS (se även punkt 3.11) Datatillsynsmannen rekommenderar därför att artikel 23.2 utgår.

Datatillsynsmannen skulle vilja understryka att det är ännu viktigare med en heltäckande beskrivning av kommissionens uppgifter avseende VIS ifall kommissionen planerar att överlåta förvaltningen till ett annat organ. I den finansieringsöversikt (”fiche financière”) som bifogas förslaget nämns möjligheten att överföra dessa uppgifter till den europeiska gränsförvaltningsbyrån. Det är här av avgörande vikt att kommissionen klargör räckvidden för sina befogenheter, eftersom efterföljaren måste känna till gränserna för sin verksamhet.

3.9 **Säkerhet**

Att VIS fungerar med en optimal säkerhetsnivå utgör en förutsättning för att det nödvändiga skydd för personuppgifter som lagras i dess databas skall säkerställas. För att uppnå en tillfredsställande nivå på skyddet måste ordentliga skyddsåtgärder införas så att de potentiella riskerna för systemets infrastruktur och de personer som är inblandade går att hantera. Denna fråga diskuteras nu i olika delar av förslaget och här behövs en viss förbättring.

Artiklarna 25 och 26 i förslaget innehåller olika åtgärder för datasäkerhet och här omnämns också de olika former av missbruk som måste förebyggas. Dessa bestämmelser kan dock med fördel kompletteras av åtgärder i syfte att systematiskt följa upp och lämna rapporter om effektiviteten hos de ovan nämnda säkerhetsåtgärderna. Datatillsynsmannen rekommenderar särskilt att dessa artiklar kompletteras med bestämmelser om systematisk (egen)kontroll av säkerhetsåtgärderna.

Detta är kopplat till artikel 40 i förslaget som innehåller bestämmelser om uppföljning och utvärdering. Detta bör inte enbart röra sådana aspekter som avser produktivitet, kostnadseffektivitet och tjänsternas kvalitet utan också efterlevnaden av rättsliga krav, särskilt på området dataskydd. Datatillsynsmannen rekommenderar därför att räckvidden för artikel 40 utsträcks till att omfatta uppföljning av och rapportering om när behandlingen av personuppgifter är laglig.

För att komplettera artikel 24.4 c eller artikel 26.2. e rörande den vederbörligen bemyndigade personal som har tillgång till uppgifterna bör det dessutom läggas till att medlemsstaterna bör säkerställa att korrekta användarprofiler finns tillgängliga (som bör hållas tillgängliga för den nationella tillsynsmyndigheterna för kontroller). Förutom dessa användarprofiler måste det finnas en komplett förteckning över användaridentiteter som ständigt hålls uppdaterad av medlemsstaterna. Detta gäller även kommissionen; artikel 25.2 b bör därför kompletteras i samma avseende.

([1]) Se sidan 37 i förslaget.

([2]) Även om definitionen av registeransvarig i direktiv 95/46/EG och förordning 45/2001 också ger en möjlighet till fler registeransvariga med olika ansvarsområden.

Dessa säkerhetsåtgärder kompletteras genom uppföljning och organisatoriska kontroller. I artikel 28 i förslaget beskrivs villkoren för och syftena med registren över all uppgiftsbehandling i VIS. Dessa register skall inte enbart lagras för uppföljning av dataskydd och säkerställande av datasäkerhet men även för regelbunden egenkontroll av VIS. Rapporterna över egenkontrollen kommer att bidra till ett effektivt genomförande av tillsynsmyndigheternas uppgifter och dessa kommer att kunna identifiera de svagaste punkterna och inrikta sig på dem under sitt eget kontrollförfarande.

3.10 **Den registrerades rättigheter**

3.10.1 *Information till den registrerade*

För att säkerställa en rättvis behandling är det ytterst viktigt att den registrerade informeras. Detta utgör ett oumbärligt skydd för den enskildes rättigheter. Artikel 30 i förslaget följer nu i princip artikel 10 i direktiv 95/46/EG i detta avseende.

Denna bestämmelse kunde dock vinna på vissa ändringar så att den bättre passar in i VIS ram. I direktivet finns bestämmelser om att viss information skall lämnas, men ger möjlighet att lämna ytterligare upplysningar om så är lämpligt ([1]). Artikel 30 bör följaktligen ändras för att omfatta följande punkter:

— Registrerade personer bör även informeras om lagringsperioden för de uppgifter som rör dem.

— Artikel 30.1 e rör ”rätten att få tillgång till och rättelse av de uppgifter som rör den personen”. Det vore lämpligare att nämna rätten att få tillgång till och att *begära* rättelse *eller radering* av de uppgifter som rör den personen. Registrerade personer bör därför informeras om möjligheten att be de berörda tillsynsmyndigheterna om råd eller hjälp.

— Slutligen nämns i artikel 30.1 a information om den registeransvariges eller dennes eventuelle ställföreträdares identitet. Eftersom den registeransvarige alltid finns etablerad inom Europeiska unionens territorium finns det inget behov av att förutse den sistnämnda möjligheten.

3.10.2 *Rätt till tillgång, korrigering och radering*

I artikel 31.1 sista meningen står det att ”Sådan tillgång till uppgifter får endast beviljas av en medlemsstat”. Detta kan antas betyda att tillgång till (eller meddelande om) uppgifterna inte kan beviljas av den centrala enheten, men däremot av vilken medlemsstat som helst. Datatillsynsmannen rekommenderar att det uttryckligen sägs att sådan information kan begäras i vilken medlemsstat som helst.

Utformningen av denna bestämmelse tycks även innebära att tillgång inte kan vägras och kommer att ges utan tillstånd från den ansvariga medlemsstaten. Detta skulle förklara varför nationella myndigheter måste samarbeta för att göra gällande de rättigheter som fastställs i artikel 31.2-4, men inte i artikel 31.1 ([2]).

3.10.3 *Hjälp från tillsynsmyndigheter*

I artikel 33.2 fastställs det att skyldigheten för de nationella tillsynsmyndigheterna att hjälpa och råda den berörda personen skall gälla under hela förfarandet (i domstol). Avsikten med denna punkt är inte klar. De nationella tillsynsmyndigheterna har olika syn på sin roll under domstolsförfarandet. Detta låter som om de måste spela rollen av rådgivare till klaganden i domstolen, vilket i många länder är omöjligt.

([1]) Där sägs ”*All ytterligare information (…) i den utsträckning som den ytterligare informationen - med hänsyn till de särskilda omständigheter under vilka uppgifterna samlas in - är nödvändig för att tillförsäkra den registrerade en korrekt behandling*”.

([2]) Artikel 31.3 om samarbete mellan nationella myndigheter vid utövandet av rätten till korrigering eller radering kunde därför för större tydlighet ändras enligt följande: ”Om den framställning *som avses i 31.2 …*”. Den framställning som avses i 31.1 (åtkomst) medför inte något samarbete mellan myndigheter.

3.11 **Tillsyn**

I förslaget fördelas tillsynsuppgiften mellan de nationella tillsynsmyndigheterna och datatillsynsmannen. Detta överensstämmer med förslagets syn på tillämplig lagstiftning och ansvar för drift och användning av VIS och med behovet av effektiv tillsyn. Datatillsynsmannen välkomnar därför detta synsätt i artiklarna 34 och 35.

De nationella tillsynsmyndigheterna följer upp frågan om när personuppgifter får behandlas av medlemsstaterna, *däribland överföringen av dem till och från VIS*. Datatillsynsmannen följer upp kommissionens verksamhet (…) *samt att personuppgifter överförs på ett lagligt sätt mellan de nationella gränssnitten och det centrala informationssystemet för viseringar*. Detta skulle kunna leda till överlappning eftersom både den nationella tillsynsmyndigheten och datatillsynsmannen samtidigt har ansvaret för tillsynen av att överföringen av personuppgifterna mellan de nationella gränssnitten och det centrala informationssystemet för viseringar är laglig.

Datatillsynsmannen föreslår därför en ändring av artikel 34 för att klargöra att den nationella tillsynsmyndigheten följer upp att medlemsstatens behandling av personuppgifter är laglig, inbegripet överföringen av dem till och från de nationella gränssnitten för VIS.

När det gäller tillsynen av VIS är det även viktigt att framhålla att de nationella tillsynsmyndigheternas och datatillsynsmannens tillsyn bör samordnas i viss mån för att säkerställa en tillräcklig grad av enhetlighet och övergripande effektivitet. Det är nödvändigt med ett harmoniserat genomförande av förordningen och att man verkar för ett gemensamt tillvägagångssätt när det gäller gemensamma problem. Eftersom det rör säkerhet kan det dessutom tilläggas att VIS säkerhetsnivå slutligen kommer att avgöras av säkerhetsnivån hos dess svagaste länk. I detta avseende behöver även samarbetet mellan datatillsynsmannen och de nationella myndigheterna struktureras och förbättras. Artikel 35 bör därför innehålla en bestämmelse om detta där det fastställs att datatillsynsmannen skall sammankalla ett möte med alla nationella tillsynsmyndigheter, minst en gång varje år.

3.12 **Genomförande**

I artikel 36.2 i förslaget föreskrivs följande: *"De föreskrifter som är nödvändiga för det tekniska genomförandet av de funktioner som avses i punkt 1 skall utfärdas i enlighet med det förfarande som avses i artikel 39.2"*. I artikel 39 hänvisas till en kommitté som skall biträda kommissionen. Kommittén inrättades i december 2001 ([1]) och har använts i flera instrument.

Det tekniska genomförandet av VIS funktioner (växelverkan med de behöriga myndigheterna och viseringens enhetliga format) innebär ett antal möjliga kritiska följder för dataskyddet. Till exempel valet att lägga in ett mikrochip i viseringen vilket kommer att få följder för hur den centrala databasen kommer att användas, liksom att standarden för det format som används för utbytet av biometriska uppgifter kommer att driva på eller utforma den dataskyddspolicy som sammanhänger med detta ([2]).

Detta val av teknik kommer att ha avgörande följder för det korrekta genomförandet av syftes- och proportionalitetsprinciperna, och bör följaktligen ses över. Val av teknik med viktiga följder för personuppgiftsskyddet bör därför helst göras genom en förordning i enlighet med medbeslutandeförfarandet. Endast då kan den nödvändiga politiska kontrollen utövas. I alla andra fall med följder för dataskyddet bör datatillsynsmannen ges möjlighet att lämna råd om de val som görs av denna kommitté.

3.13 **Interoperabilitet**

En viktig och avgörande förutsättning för att storskaliga system som VIS skall bli effektiva är interoperabilitet. Den ger möjlighet att konsekvent minska de totala kostnaderna och att undvika en naturlig överlappning av heterogena delar. Interoperabilitet kan även bidra till målet att åstadkomma en gemensam viseringspolitik genom att tillämpa samma normer för förfarandet för alla bärande delar av denna politik. Det är dock mycket viktigt att skilja mellan följande två nivåer för interoperabilitet:

— Interoperabilitet mellan EU:s medlemsstater är högst önskvärd; viseringsansökningar som sänds från en medlemsstats myndigheter måste vara interoperabla med sådana som översänts av alla andra staters myndigheter.

([1]) Rådets förordning nr 2424/2001 av den 6 december 2001 om utvecklingen av andra generationen av Schengens informationssystem (SIS II).

([2]) Förslaget till rådets förordning om ändring av (EG) 1683/95 (enhetlig utformning av visumhandlingar) från september 2003 innefattar även en liknande artikel.

— Behovet av interoperabilitet mellan system som konstruerats för olika ändamål eller med tredjelandssystem kan däremot ifrågasättas.

Som exempel på tillgängliga skyddsåtgärder som används för att begränsa systemets syfte och förebygga ”funktionsglidning” kan nämnas användningen av olika tekniska normer som bidrar till denna begränsning. Dessutom bör alla slag av interaktion mellan två olika system dokumenteras noggrant. Interoperabilitet bör aldrig leda till ett läge där en myndighet som inte har rätt till tillgång eller användning av vissa uppgifter kan erhålla dessa via ett annat informationssystem.

I detta sammanhang skulle datatillsynsmannen vilja hänvisa till rådets uttalande av den 25 mars 2004 om kamp mot terrorism, där kommissionen uppmanas att lägga fram förslag i syfte att öka interoperabilitet och samverkan mellan informationssystem (SIS, VIS och Eurodac).

Datatillsynsmannen skulle även vilja hänvisa till den pågående diskussionen om vilket organ som kan anförtros förvaltningen av de olika storskaliga systemen i framtiden (se även punkt 3.8 i detta yttrande).

Datatillsynsmannen vill återigen betona att systemens interoperabilitet inte kan genomföras i strid mot principen om begränsning av syftet och att alla förslag i frågan bör läggas fram för honom.

4. SLUTSATSER

4.1 Allmänna synpunkter

1. Datatillsynsmannen erkänner att den vidare utvecklingen av en gemensam viseringspolitik kräver ett effektivt utbyte av relevanta uppgifter. En av de mekanismer som kan garantera ett jämnt flöde av information är VIS. Datatillsynsmannen har noggrant noterat de bevis som läggs fram i den utvidgade konsekvensanalysen. Även om dessa bevis inte är avgörande verkar det finnas tillräckliga skäl för att motivera att VIS inrättas i syfte att förbättra den gemensamma viseringspolitiken.

   Detta nya instrument bör dock begränsas till insamlande och utbyte av uppgifter, i den mån som det behövs insamlande och utbyte för att utveckla en gemensam viseringspolicy och det står i rimlig proportion till detta mål.

2. Inrättandet av VIS kan få positiva följder för andra legitima allmänna intressen, men detta ändrar inte syftet med VIS. Därför måste alla inslag i VIS vara nödvändiga och proportionerliga instrument för att nå det ovannämnda målet för policyn. Till detta kan läggas att

   — det inte skulle vara förenligt med detta syfte att ge de brottsförebyggande myndigheterna rutinmässig tillgång,

   — datatillsynsmannen rekommenderar att denna skillnad mellan syfte och nytta uttrycks klarare i artikel 1.2,

   — interoperabilitet med andra system inte kan genomföras i strid med principen om begränsning av ändamålet.

3. Datatillsynsmannen inser fördelarna med användningen av biometriska uppgifter, men betonar de allvarliga följderna av användningen av sådana uppgifter och föreslår att kraftfulla skyddsåtgärder införs för användningen av biometriska uppgifter. De tekniska bristerna hos fingeravtryck kräver att reservförfaranden utarbetas och innefattas i förslaget.

4. Detta yttrande bör nämnas i förordningens ingress före skälen (”med beaktande av yttrandet …”).

4.2 **Övriga synpunkter**

5. När det gäller grunderna för avslag av viseringsansökningar bör en hänvisning till artikel 29 i direktiv 2004/58/EG införas i förslaget för att säkerställa att ”hot mot folkhälsan” ses mot bakgrund av den bestämmelsen.

6. Uppgifter om gruppmedlemmar har en särskild betydelse i förslaget och en tydlig och övergripande definition av ”gruppmedlem” bör därför ges.

7. Det finns inget som tyder på att valet av policy i detta förslag när det gäller tidsfristen för lagring av uppgifter är orimlig eller skulle få oacceptabla följder, förutsatt att det finns lämpliga mekanismer för korrigering.

   Det bör dessutom klart anges i förslaget att det måste göras en ny helt bedömning av personuppgifterna för varje ny viseringsansökan.

8. När det gäller viseringskontroller vid yttre gränser bör artikel 16 i förslaget ändras eftersom tillgång till VIS centrala databas i dessa fall skulle vara orimlig. Det skulle räcka med att den behöriga myndigheten fick tillgång till det skyddade mikrochipet och därmed kunde utföra viseringskontroller.

   Om identiteten har kontrollerats, är det mycket oklart varför övriga uppgifter skulle behövs.

9. När det gäller uppgifter för identifiering och återsändande av olagliga invandrare och för asylförfaranden bör ”fotografier” tas bort från första delen av artiklarna 17-19 men däremot stå kvar i andra delen.

10. När det gäller kommissionens och medlemsstaternas ansvar bör artikel 23.2 strykas.

11. Bestämmelser om systematiska (egen)kontroller av säkerhetsbestämmelser bör läggas till i förslaget. Räckvidden för artikel 40 måste utvidgas till att omfatta uppföljning av och rapportering om när behandling av personuppgifter är laglig. Det finns också behov av följande:

   — En komplett förteckning över användaridentiteter måste upprättas och hållas ständigt uppdaterad av medlemsstaterna. Detta gäller även kommissionen och artikel 25.2 b bör därför kompletteras på samma sätt.

   — I artikel 28 i förslaget beskrivs villkoren för att föra register och för vilka syften register över all uppgiftsbehandling i VIS måste föras. Dessa register skall inte enbart lagras för övervakning av dataskydd och säkerställande av datasäkerhet men även för regelbunden egenkontroll av VIS.

12. När det gäller den registrerades rättigheter bör

   — artikel 30 ändras i syfte att säkerställa att registrerade personer även informeras om den lagringsperiod som gäller för deras uppgifter,

   — det i artikel 30.1 e nämnas ”rättigheter att få tillgång till och att begära rättelse eller radering av uppgifter”,

   — det i artikel 31.1 uttryckligen anges att sådan information kan begäras i vilken medlemsstat som helst.

13. När det gäller tillsyn bör

— artikel 34 ändras så att det klargörs att den nationella tillsynsmyndigheten följer upp att medlemsstatens behandling av personuppgifter är laglig, inbegripet överföringen av dem till och från de nationella gränssnitten för VIS,

— artikel 35 innehålla en bestämmelse där det fastställs att datatillsynsmannen skall sammankalla ett möte med alla nationella tillsynsmyndigheter, minst en gång varje år.

14. När det gäller genomförandet bör

— valet av teknik med allvarliga följder för dataskyddet helst göras genom en förordning i enlighet med medbeslutandeförfarandet,

— datatillsynsmannen i andra fall ges möjlighet att ge råd om de val som gjorts av den kommitté som avses i förslaget.

Bryssel den 23 mars 2005

Peter HUSTINX

Europeiska datatillsynsmannen