EUROPEISKA DATATILLSYNSMANNEN

Yttrande från Europeiska datatillsynsmannen

— om förslaget till rådets beslut om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) (KOM(2005) 230 slutlig),

— om förslaget till Europaparlamentets och rådets förordning om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) (KOM(2005) 236 slutlig), och

— om förslaget till Europaparlamentets och rådets förordning om tillträde till andra generationen av Schengens informationssystem (SIS II) för de enheter i medlemsstaterna som ansvarar för att utfärda registreringsbevis för fordon (KOM(2005) 237 slutlig).

(2006/C 91/11)

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, särskilt artikel 41,

med beaktande av den begäran om ett yttrande i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 som mottogs den 17 juni 2005 från kommissionen.

HÄRIGENOM FRAMFÖRS FÖLJANDE.

1. INLEDNING

1.1 Bakgrund

Schengens informationssystem (SIS) är ett storskaligt IT-system för EU som inrättats som en kompensationsåtgärd till följd av avskaffandet av kontrollerna vid de inre gränserna inom Schengenområdet. SIS ger behöriga myndigheter i medlemsstaterna möjlighet att utbyta information som används för att genomföra kontroller av personer och föremål vid de yttre gränserna eller på territoriet och för att utfärda viseringar och uppehållstillstånd.

Schengenkonventionen trädde i kraft 1995 som ett mellanstatligt avtal. SIS som är en del av Schengenkonventionen införlivades senare inom EU:s ram genom Amsterdamfördraget.

En ny ”andra generation” av Schengens informationssystem (SIS II) kommer att ersätta det nuvarande systemet och därigenom möjliggöra utvidgningen av Schengenområdet till de nya EU-medlemsstaterna. Det kommer också att införas nya funktioner i systemet. Schengen-bestämmelserna, som utformats inom en mellanstatlig ram, kommer att införlivas fullt ut i traditionella europeiska lagstiftningsinstrument.

Den 1 juni 2005 lade Europeiska kommissionen fram tre förslag till inrättande av SIS II. Dessa förslag består av

— ett förslag till förordning, som grundas på avdelning IV i EG-fördraget (visering, asyl och invandring och annan politik som rör fri rörlighet för personer) och som kommer att reglera de aspekter av SIS som rör första pelaren (invandring), nedan kallat förslaget till förordning,

— ett förslag till beslut, som grundas på avdelning VI i EU-fördraget (polissamarbete och straffrättsligt samarbete) och som kommer att reglera användningen av SIS för syften som rör tredje pelaren, nedan kallat förslaget till beslut,

— ett förslag till förordning som grundas på avdelning V (transporter) och specifikt rör tillträde till uppgifter i SIS för myndigheter som utfärdar registreringsbevis för fordon. Detta förslag kommer att behandlas separat (se nedan, punkt 4.6).

Det är värt att nämna i detta sammanhang att kommissionen under de kommande månaderna kommer att utfärda ett meddelande om interoperabilitet och ökade synergier mellan EU:s informationssystem (SIS, VIS och Eurodac).

SIS II består av en central databas som kallas Schengens centrala informationssystem (CS-SIS), för vilken kommissionen kommer att sörja för den operativa förvaltning som är kopplad till nationella anslutningspunkter som skall fastställas av de enskilda medlemsstaterna (NI-SIS). Sirenemyndigheter skall sörja för utbytet av kompletterande information (information som har anknytning till SIS II-rapporter men som inte lagras i SIS II).

Medlemsstaterna kommer att bidra med uppgifter till SIS II om personer som efterlyses för att häktas, överlämnas eller utlämnas, personer som efterlyses för att lagföras, personer som skall sättas under övervakning eller utsättas för särskilda kontroller, personer som skall nekas inresa vid den yttre gränsen samt försvunna eller stulna föremål. En uppsättning uppgifter som kallas ”rapporter” och som införs i SIS gör det möjligt för den behöriga myndigheten att identifiera en person eller ett föremål.

I SIS II utvecklas nya egenskaper: utökat tillträde till SIS (Europol, Eurojust, nationella åklagare, myndigheter som utfärdar registreringsbevis för fordon), sammankoppling av rapporter, tillägg av nya kategorier av uppgifter, inklusive biometriska uppgifter (fingeravtryck och foton) samt en teknisk plattform som skall delas med Informationssystemet för viseringar. Dessa tillägg har orsakat diskussioner i flera år om en ändring av syftet med SIS, från ett kontrollverktyg till ett system för rapportering och undersökning.

1.2 **Allmän bedömning av förslagen**

1. Datatillsynsmannen välkomnar att han blir föremål för samråd på grundval av artikel 28.2 i förordning (EG) nr 45/2001. Eftersom artikel 28.2 är tvingande bör emellertid detta yttrande omnämnas i ingressen till rättsakterna.

2. Av flera skäl välkomnar datatillsynsmannen förslagen. Att införliva en mellanstatlig struktur i europeiska lagstiftningsinstrument medför flera positiva följder: det rättsliga värdet av reglerna för SIS II kommer att klargöras, domstolen kommer att få behörighet att tolka det rättsinstrument som rör första pelaren, Europaparlamentet blir åtminstone delvis inbegripet (även om det sker något sent i processen).

3. I sak ägnas dessutom en betydande del av förslagen åt uppgiftsskydd, och en del av detta är välkomna förbättringar jämfört med den nuvarande situationen. Man kan särskilt nämna åtgärderna för personer som utsatts för identitetsstöld, utvidgningen av förordning nr 45/2001 till att även gälla det fall då kommissionen behandlar uppgifter inom ramen för verksamheten inom avdelning VI och en bättre definition av skälen för registrering av enskilda personer i syfte att vägra inresa.

4. Det är också uppenbart att stor omsorg har ägnats åt utformningen av förslagen. De är komplexa, men detta speglar den komplexa beskaffenheten hos själva det system som de skall reglera. De flesta kommentarerna i detta yttrande syftar till att klargöra eller komplettera bestämmelser men innebär inte att det krävs någon fullständig omarbetning.

Trots denna allmänt sett positiva bedömning kan dock vissa reservationer göras beträffande bland annat följande:

1. Det är i många hänseenden svårt att veta vilken avsikt som ligger bakom texten. Det är mycket beklagligt att det saknas en motivering. Eftersom dessa dokument är mycket komplexa till sin natur skulle detta har varit ett grundläggande krav. Avsaknaden av en motivering gör att läsaren i vissa fall inte har något annat alternativ än att gissa.

2. Dessutom kan det endast beklagas att ingen konsekvensbedömning har genomförts. Det faktum att den första versionen av systemet redan har införts rättfärdigar inte detta eftersom det finns avsevärda skillnader mellan de båda. Till exempel borde effekterna av införandet av biometriska uppgifter ha undersökts bättre.

3. Den rättsliga ramen för uppgiftsskydd är mycket komplex. Den grundas på en kombinerad tillämpning av *lex generalis* (generell lagstiftning) och *lex specialis* (specifik lagstiftning). Det bör säkerställas att den befintliga ramen för uppgiftsskydd i direktiv 95/46/EG och förordning nr 45/2001 förblir tillämplig fullt ut även när en specifik lagstiftning utformas. En kombinerad tillämpning av olika rättsinstrument bör inte leda vare sig till olikheter mellan nationella ordningar när det gäller grundläggande aspekter eller till en urvattning av den nuvarande nivån på uppgiftsskyddet.

4. Eftersom många nya myndigheter som inte passar in i det ”ursprungliga syftet med kontrollerna av personer och föremål” får tillträde till systemet, bör strängare skyddsgarantier införas.

5. Förslagen grundas till betydande del på andra rättsinstrument som fortfarande är under utarbetande (beträffande vilka det ibland inte ens har lagts fram förslag). Datatillsynsmannen inser svårigheterna med att lagstifta i en komplex miljö i ständig utveckling, men med hänsyn till följderna för de berörda personerna och till den rättsosäkerhet som det medför anser han det oacceptabelt.

6. Det råder viss oklarhet om fördelningen av befogenheter mellan medlemsstaterna och kommissionen. Tydlighet är ytterst viktigt eftersom detta inte bara är nödvändigt för att systemet skall fungera väl utan också är ett grundläggande krav för att säkerställa en övergripande tillsyn av systemet.

1.3 **Yttrandets struktur**

Yttrandet kommer att struktureras på följande sätt: Först klargörs den rättsliga ramen för SIS II. Därefter behandlas definitionen av syftet med SIS II och de delar som avsevärt skiljer sig från det nuvarande systemet. Punkt 5 innehåller kommentarer om kommissionens och medlemsstaternas respektive roller i driften av SIS II. Punkt 6 rör den registrerades rättigheter och punkt 7 behandlar tillsynen, på nationell nivå och från datatillsynsmannens sida, samt samarbetet mellan tillsynsmyndigheterna. I punkt 8 framläggs vissa synpunkter och möjliga ändringar i fråga om säkerheten. I punkterna 9 och 10 behandlas kommittéförfarande respektive interoperabilitet. I en sammanfattning av slutsatserna framläggs slutligen de viktigaste slutsatserna för varje punkt.

2. **RELEVANT RÄTTSLIG RAM**

2.1 **Relevant ram för uppgiftsskydd när det gäller SIS II**

I förslagen anges direktiv 95/46/EG, (Europarådets) konvention nr 108 och förordning nr 45/2001 som förslagens rättsliga ram för uppgiftsskydd. Andra instrument är också relevanta.

För att klargöra detta sammanhang och erinra om vilka de viktigaste referenspunkterna för vår granskning är, är det lämpligt att ta upp följande:

— Respekten för privatlivet har varit garanterad i Europa sedan Europarådet 1950 antog konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (nedan kallad ECHR). I artikel 8 i ECHR fastställs att var och en har ”rätt till skydd för sitt 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 ingripanden, åtgärdernas proportionalitet och behovet av lämpliga skyddsåtgärder mot missbruk.

— Rätten till respekt för privatliv och skydd av personuppgifter har på senare tid fastställts i artiklarna 7 och 8 i Europeiska unionens stadga om de mänskliga rättigheterna. Enligt artikel 52 i stadgan erkänns att dessa rättigheter kan begränsas under förutsättning att villkor som är likvärdiga med dem i artikel 8 i ECHR är uppfyllda.

— I artikel 6.2 i EU-fördraget fastställs att unionen skall respektera de grundläggande rättigheterna, såsom de garanteras i Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

Följande tre rättsakter är klart tillämpliga på förslagen om SIS II:

— Europarådets konvention nr 108 av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter (nedan kallad konvention nr 108) innehåller grundläggande principer för skydd för enskilda vid automatisk databehandling av personuppgifter. Samtliga medlemsstater har ratificerat konvention nr 108. Den är även tillämplig på verksamheter som bedrivs inom ramen för de polisiära och rättsliga områdena. Konvention nr 108 är för närvarande den ordning för uppgiftsskydd som är tillämplig på SIS-konventionen, tillsammans med rekommendation nr R (87) 15 av den 17 september 1987 från Europarådets ministerkommitté om polisens användning av personuppgifter.

— 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 kallas nedan direktiv 95/46/EG. Det är värt att notera att den nationella lagstiftningen om genomförandet av direktivet i de flesta medlemsstaterna även omfattar den behandling av uppgifter som utförs av polis och rättsväsen.

— 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 kallas nedan förordning nr 45/2001.

Direktiv 95/46/EG och förordning nr 45/2001 måste delvis tolkas med hänsyn till relevant rättspraxis vid Europeiska domstolen för de mänskliga rättigheterna i enlighet med den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (ECHR) från 1950. Med andra ord måste direktivet och förordningen, i den mån de handlar om behandling av personuppgifter som kan kränka grundläggande friheter och i synnerhet rätten till privatliv, tolkas mot bakgrund av de grundläggande rättigheterna. Detta följer också av rättspraxis vid Europeiska gemenskapernas domstol ([1]).

([1]) Det är lämpligt att i detta sammanhang hänvisa till domstolens dom i målet Österreichischer Rundfunk m.fl. (Förenade mål C-465/00, C-138/01 och C-139/01, dom av den 20 maj 2003, sammanträde i plenum, (2003) REG I-4989). Domstolen behandlade en österrikisk lag om överföring av löneuppgifter för offentliganställda till den österrikiska revisionsrätten och det därpå följande offentliggörandet av dessa uppgifter. I sin dom fastslår domstolen ett antal kriterier från artikel 8 i ECHR som bör användas vid tillämpningen av direktiv 95/46/EG i den mån det i detta direktiv anges vissa begränsningar av rätten till privatliv.

Den 4 oktober 2005 utfärdade kommissionen ett förslag till rådets rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete ([1]) (nedan kallat utkastet till rambeslut). Detta rambeslut är avsett att ersätta konvention nr 108 som referenslagstiftning för utkastet till beslutet om SIS II, vilket troligen kommer att få följder för ordningen för uppgiftsskydd i detta sammanhang (se nedan, punkt 2.2.5).

2.2 **Rättsordning för uppgiftsskydd när det gäller SIS II**

2.2.1 *Allmän anmärkning*

Den rättsliga grunden för SIS II består av separata instrument men, såsom anges i ingressen, detta ”påverkar inte principen att SIS II är ett enda system som skall fungera som ett enda system. Vissa av bestämmelserna i dessa instrument bör därför vara identiska.”

De båda dokumentens struktur är i grunden den samma och kapitlen I–III är rent av nästan identiska i båda texterna. Det faktum att SIS II skall betraktas som ett enda informationssystem med två olika rättsliga grunder speglas också i – den tämligen komplexa – ordningen för uppgiftsskydd.

Ordningen för uppgiftsskydd fastställs delvis i själva förslagen, som en *lex specialis* som kompletteras genom en annan referenslagstiftning (*lex generalis*) för varje avsnitt (kommissionen, medlemsstaterna i första pelaren, medlemsstaterna i tredje pelaren).

Denna struktur ger upphov till frågan om hur specifika uppsättningar av regler skall behandlas i förhållande till allmän lagstiftning. I detta fall anser datatillsynsmannen att den särskilda regeln är en tillämpning av den allmänna regeln. Därför måste *lex specialis* alltid stå i överensstämmelse med *lex generalis*. Den är en vidareutveckling (specificering eller utökning) av *lex generalis* men är inte att betrakta som ett undantag från den.

När det gäller frågan om vilken regel som bör tillämpas i specifika fall är principen att *lex specialis* skall tillämpas med förtur, men när den lagen tiger eller är oklar bör hänvisning göras till *lex generalis*.

Enligt denna struktur finns det tre olika kombinationer av *lex generalis* och *lex specialis*. Det kan sammanfattas på följande sätt:

2.2.2 *Tillämplig ordning för kommissionen*

Om kommissionen är inblandad är förordning 45/2001 tillämplig, inklusive datatillsyningsmannens roll, vare sig verksamheterna utförs inom ramen för första (förslaget till förordning) eller tredje pelaren (förslaget till beslut). I skäl 21 i förslaget till beslut anges följande: ”förordning (EG) nr 45/2001 (…) skall tillämpas då kommissionen behandlar personuppgifter, i de fall då behandlingen görs för att utföra uppgifter som helt eller delvis omfattas av gemenskapslagstiftningen. Behandlingen av personuppgifter inom SIS II omfattas till viss del av gemenskapslagstiftningen”.

Det finns praktiska skäl för detta: det skulle verkligen vara ytterst svårt att när det gäller kommissionen fastställa om uppgifterna behandlas inom ramen för verksamhet som faller inom lagstiftningen för första eller tredje pelaren.

Att tillämpa ett rättsinstrument på all verksamhet som kommissionen utför inom ramen för SIS II är dessutom inte bara mer rimligt ur praktisk synvinkel, utan det förbättrar också enhetligheten (och säkerställer enligt skäl 21 i förslaget till förordning en ”konsekvent och enhetlig tillämpning av reglerna om skydd av individens grundläggande rättigheter och friheter i samband med behandlingen av personuppgifter”). Datatillsynsmannen välkomnar därför kommissionens erkännande av att förordning nr 45/2001 är tillämplig på all behandling av personuppgifter som kommissionen utför i SIS II.

2.2.3 *Tillämplig ordning för medlemsstaterna*

Situationen är mer komplex när det gäller medlemsstaterna. Behandlingen av personuppgifter i enlighet med förslaget till förordning regleras av själva förslaget till förordning samt av direktiv 95/46/EG. Av lydelsen i skäl 14 i förslaget till förordning framgår mycket tydligt att direktivet måste anses som *lex generalis* medan förordningen om SIS II kommer att vara *lex specialis*. Detta får en del konsekvenser som beskrivs närmare nedan.

När det gäller förslaget till beslut är det rättsliga referensinstrumentet för uppgiftsskydd (*lex generalis*) konvention nr 108, vilket kan göra en viktig skillnad mellan ordningarna för uppgiftsskydd inom första och tredje pelaren på några punkter.

2.2.4 *Inverkan på uppgiftsskyddet*

Som en allmän kommentar till denna uppbyggnad av uppgiftsskyddet understryker datatillsynsmannen följande:

— Tillämpningen av den föreslagna förordningen som en *lex specialis* av direktiv 95/46/EG (och på liknande sätt av det föreslagna beslutet som en *lex specialis* av konvention nr 108) bör aldrig leda till en urvattning av det uppgiftsskydd som garanteras enligt direktivet eller konventionen. Datatillsynsmannen kommer att lämna rekommendationer om detta (se exempelvis rätten till rättsmedel).

([1]) (KOM(2005) 475 slutlig).

— På liknande sätt får den kombinerade tillämpningen av rättsliga instrument inte leda till att det uppgiftsskydd som garanteras enligt den nuvarande Schengenkonventionen försämras (se exempelvis kommentarerna nedan till artikel 13 i direktiv 95/46/EG).

— Tillämpningen av två olika instrument, även om det är nödvändigt på grund av den europeiska rättsliga ramen, bör inte leda till omotiverade avvikelser mellan de berörda enskilda personernas uppgiftsskydd alltefter den typ av uppgifter om dem som behandlas. Detta måste undvikas så långt som möjligt. Syftet med rekommendationerna nedan är också att förbättra enhetligheten så mycket som möjligt (se exempelvis de nationella tillsynsmyndigheternas befogenheter).

— Den rättsliga ramen är så komplex att den med all sannolikhet kommer att skapa en del förvirring vid den praktiska tillämpningen. Det är i en del fall svårt att se hur *lex generalis* och *lex specialis* påverkar varandra, och det skulle vara bra om detta klargörs i förslagen. I detta komplexa rättsliga sammanhang är förslaget från den gemensamma tillsynsmyndigheten för Schengen i dess ”yttrande om den föreslagna rättsliga grunden för SIS II” (den 27 september 2005) om att utveckla ett ”vademecum”, där alla rättigheter som finns när det gäller SIS II uppräknas och där en tydlig hierarki anges för tillämplig lagstiftning, mycket konstruktivt.

Sammanfattningsvis är syftet med detta yttrande att säkerställa en hög nivå på uppgiftsskydd, enhetlighet och klarhet för att ge den registrerade nödvändig rättssäkerhet.

2.2.5 *Inverkan från utkastet till rambeslut om skydd av personuppgifter inom tredje pelaren*

Konvention nr 108 som är referensinstrumentet när det gäller uppgiftsskydd för utkastet till beslut om SIS II kommer att ersättas av rambeslutet om skydd av personuppgifter inom tredje pelaren ([1]). Detta nämns inte i förslaget, men är en följd av den föreslagna rambeslutet. I artikel 34.2 i rambeslutet anges att ”Varje hänvisning till Europarådets konvention nr 108 av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter skall förstås som en hänvisning till detta rambeslut”. Datatillsynsmannen kommer inom de närmaste veckorna att yttra sig om utkastet till rambeslut och kommer inte att i detalj analysera dess innehåll i detta yttrande. Om tillämpningen av rambeslutet kan komma att få en betydande inverkan på ordningen för uppgiftsskydd i SIS II kommer detta dock att nämnas.

([1]) Det kommer också att ersätta den allmänna ordningen för uppgiftsskydd i Schengenkonventionen (artiklarna 126–130 i Schengenkonventionen). Ordningen gäller inte för SIS.

2.2.6 *Tillämpning av artikel 13 i direktiv 95/46/EG och artikel 9 i konvention 108*

Enligt artikel 13 i direktiv 95/46/EG och artikel 9 i konvention 108 får medlemsstaterna genom lagstiftning vidta åtgärder för att begränsa omfattningen av de skyldigheter och rättigheter som anges för dem i fall då en sådan begränsning är en nödvändig åtgärd för att skydda andra viktiga intressen (t.ex. statens säkerhet, försvaret, allmän säkerhet) ([2]).

I skälen i både förslaget till förordning och förslaget till beslut anges att medlemsstaterna kan använda sig av denna möjlighet när de genomför förslagen på nationell nivå. Ett dubbelt test bör göras i detta fall: tillämpningen av artikel 13 i direktiv 95/46/EG måste överensstämma med artikel 8 i Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och bör inte leda till att den nuvarande ordningen för uppgiftsskydd försvagas.

Det är ännu viktigare när det gäller SIS II eftersom systemet måste vara förutsägbart. Eftersom medlemsstaterna utbyter uppgifter måste det finnas en möjlighet att med rimlig säkerhet få veta hur de kommer att behandlas på nationell nivå.

Det finns särskilt en oroande faktor när det gäller detta, nämligen att förslagen skulle leda till att den nuvarande nivån på uppgiftsskyddet sänks. Enligt artikel 102 i Schengenkonventionen skall det finnas ett system i vilket användningen av uppgifter är strikt reglerad och begränsad även i nationell lagstiftning (”All användning av uppgifterna som inte är förenlig med punkterna 1–4 skall betraktas som åsidosättande av varje parts lagar”). Både i direktiv 95/46/EG och i konvention nr 108 anges dock att undantag, bl.a. från principen om begränsning av syftet, kan införas i nationell lagstiftning. Om detta görs skulle det innebära en avvikelse från det nuvarande systemet i Schengenkonventionen, där nationell lagstiftning inte får avvika från den centrala principen om begränsning av syftet och användningen.

Denna synpunkt skulle inte ändras genom antagandet av rambeslutet: problemet ligger mycket mer i att behålla en princip om strikt begränsning av syftet för behandlingen av SIS II-uppgifter än i att säkerställa att uppgifter behandlas i enlighet med rambeslutet.

([2]) En medlemsstat som använder detta alternativ för att begränsa rättigheter får göra detta endast i enlighet med artikel 8 i Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, såsom nämnts tidigare.

Datatillsynsmannen föreslår att det i förslagen om SIS II (dvs. i artikel 21 i förslaget till förordning och artikel 40 i förslaget till beslut) införs en bestämmelse med samma verkan som den nuvarande artikel 102.4 i Schengenkonventionen, där medlemsstaternas möjlighet att tillåta användning av uppgifterna som inte förutses i texterna om SIS II begränsas. En annan möjlighet är att i förslaget till beslut och förslaget till förordning uttryckligen begränsa omfattningen av de undantag som kan tillämpas enligt artikel 13 i direktivet eller artikel 9 i konventionen och föreskriva t.ex. att medlemsstaterna endast kan begränsa rätten till tillgång och information men inte principerna om uppgiftskvalitet.

3. SYFTE

Enligt artikel 1 i de båda dokumenten (”Inrättande av SIS II och allmänt mål”) skall SIS II inrättas ”för att möjliggöra samarbete mellan medlemsstaternas behöriga myndigheter i form av utbyte av information för kontroller av personer och föremål” och skall ”bidra till en hög säkerhetsnivå inom ett område utan kontroller vid medlemsstaternas inre gränser”.

Syftet med SIS II formuleras i ganska grova drag; de ovannämnda bestämmelserna är inte i sig en exakt indikation på vad som omfattas av (avses med) detta mål.

Syftet med SIS II förefaller vara mycket vidare än syftet med det nuvarande SIS enligt artikel 92 i Schengenkonventionen, i vilken det särskilt hänvisas till ”(…) kunna få rapporter om personer och föremål för gränskontroller, undersökningar och andra kontroller som utförs av polis och tullmyndigheter (…) och (beträffande rapporter enligt artikel 96) vid utfärdande av viseringar, uppehållstillstånd och handhavande av utlänningar (…)”.

Detta vidare syfte härrör också från tillägget till SIS II av nya funktioner och ny tillgång som inte passar in i det ursprungliga syftet med kontroller av personer och föremål, men passar bättre i ett utredande verktyg. I synnerhet förutses tillgång för myndigheter som vill använda SIS II-uppgifter för egna ändamål och inte för att förverkliga SIS II-syften (se nedan); rapporter kommer generellt att kopplas samman, medan detta är ett särdrag utmärkande för ett verktyg för polisutredningar.

Det finns också frågor om den biometriska sökmotor som skall utvecklas under de kommande åren och som kommer att göra det möjligt att göra sökningar i systemet, vilka går utöver vad som behövs för ett kontrollsystem.

Förslagen har alltså en mycket vidare räckvidd än den befintliga ramen. Detta kräver ytterligare skyddsåtgärder. Datatillsynsmannen kommer i detta avseende att inrikta sin analys mer på funktionerna och de andra konstruktiva delarna av SIS II än på den breda definitionen i artikel 1.

4. BETYDANDE ÄNDRINGAR I SIS II

Detta kapitel kommer främst att inriktas på de nya inslag som införts genom SIS II, nämligen införandet av biometriska uppgifter, den nya uppfattningen om tillgång, med särskild inriktning på Europols och Eurojusts tillgång, på myndigheter med ansvar för fordonsregistrering, sammankopplingen av rapporter och olika myndigheters tillgång till uppgifter om invandring.

4.1 Biometriska uppgifter

I SIS II-förslagen införs möjligheten att behandla en ny kategori uppgifter som förtjänar särskild uppmärksamhet: biometriska uppgifter. Såsom redan framhållits i datatillsynsmannens yttrande om informationssystemet för viseringar ([1]), kräver de biometriska uppgifternas känsliga natur särskilda skyddsåtgärder som inte har införts i SIS II-förslagen.

Det kan generellt sägas att tendensen att använda biometriska uppgifter i informationssystem som omfattar hela EU (VIS, Eurodac, informationssystem om körkort osv.) stadigt ökar, men inte följs av ett noggrant övervägande av involverade risker och nödvändiga säkerhetsåtgärder.

Detta behov av en djupare eftertanke har även framhållits i resolutionen nyligen om biometriska uppgifter, som utfärdats vid dataskyddsmyndigheternas internationella konferens i Montreux ([2]). Mervärdet för utvecklingen av normer har hittills inriktats endast på den allt större kompatibiliteten mellan system och inte på en förbättring av kvaliteten på de biometriska processerna.

([1]) Punkt 3.4 2. i datatillsynsmannens 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.

([2]) Den 27:e internationella konferensen i Montreux den 16 september 2005 mellan myndigheterna för skydd av personuppgifter och skydd av privatlivet; resolution om användning av biometriska uppgifter i pass, identitetskort och resehandlingar.

Det skulle vara lämpligt att ställa upp en rad allmänna skyldigheter eller krav relaterade till sådana uppgifters särdrag samt en allmän metod för deras genomförande. I dessa allmänna krav kan särskilt följande inslag ingå (behovet av dessa illustreras i SIS II-förslagen):

— **Riktad konsekvensanalys**: Det måste understrykas att förslagen inte har varit föremål för någon konsekvensanalys av användningen av biometriska uppgifter ([1]).

— **Betoning på registreringsprocessen**: Källan till biometriska uppgifter och det sätt på vilket de kommer att samlas in beskrivs inte i detalj. Registrering är ett mycket viktigt steg i den övergripande processen med biometrisk identifiering och kan inte fastställas endast i bilagor eller under ytterligare diskussioner i undergrupper, eftersom den direkt kommer att påverka slutresultatet av processen, dvs. frekvensen av felaktiga avvisningar eller felaktiga godkännanden.

— **Framhävande av graden av korrekthet**: Användningen av biometriska uppgifter för identifiering (jämförelse av en grupp av uppgifter mot många – *"one to many"*), som lades fram i förslaget som ett framtida genomförande av en "biometrisk sökmotor", är farligare eftersom resultaten av denna process är mindre korrekta än användningen för äkthet eller kontroll (jämförelse av en grupp av uppgifter mot en annan). Biometrisk identifiering bör därför inte vara det enda identifieringssättet eller den enda nyckeln till ytterligare information.

— **Säkerhetsförfarande**: Lättillgängliga säkerhetsförfaranden skall tillämpas för att respektera värdigheten hos människor som kan ha utsatts för felaktig identifiering och för att undvika att den börda som systemets brister medför överförs på dem.

Användningen av biometriska uppgifter utan en lämplig föregående bedömning avslöjar även en övervärdering av de biometriska uppgifternas tillförlitlighet. Biometriska uppgifter är "levande" uppgifter som utvecklas med tiden och de prov som lagras i databasen är bara ett "snapshot" av ett dynamiskt element. Det har ingen absolut beständighet och måste kontrolleras. Korrektheten hos biometriska uppgifter måste sättas i relation till andra uppgifter eftersom den aldrig kommer att vara absolut.

([1]) Analysen kan bygga på den biometriska vishetens s.k. sju pelare i "Biometrics at the frontiers: Assessing the impact on Society", Institutet för prospektiva tekniska studier, Gemensamma forskningscentret, EUR 21585 EN, del 1.2, s. 32.

Eventuell användning av SIS II-uppgifter för utredningsändamål medför allvarliga risker för den registrerade om man ger biometriska bevis en ökad eller övervärderad roll, vilket har illustrerats i tidigare fall ([2]).

I förslagen bör man därför erkänna och öka medvetenheten om biometriska uppgifters verkliga kapacitet för identifieringsändamål.

4.2 **Tillgång till uppgifter i SIS II**

4.2.1 *En ny vision av tillgång*

De myndigheter som har tillgång till uppgifter i SIS preciseras för varje rapport. I princip används ett dubbelt test för beviljande av tillgång till uppgifter i SIS: tillgång måste beviljas myndigheter i full överensstämmelse med SIS allmänna syfte och med det specifika syftet med varje rapport.

Detta följer av definitionen av rapporter i både förslaget till förordning och förslaget till beslut (artikel 3.1 a i båda instrumenten: *"registrering: ett antal uppgifter som lagts in i SIS II och med hjälp av vilka de behöriga myndigheterna kan identifiera en person eller ett föremål med avsikt på en specifik åtgärd som skall vidtas"*). Artikel 39.3 förstärker den uppfattningen genom att följande anges: *"De uppgifter som avses i punkt 1 skall endast användas för identifiering av en person med avseende på en specifik åtgärd som vidtas i enlighet med detta beslut"*. I detta avseende har SIS II fortfarande de kännetecken som utmärker ett "träff/ej träff"-system, där varje rapport införs för ett specifikt syfte (överlämnande, vägrad inresa …).

De myndigheter som har tillgång till SIS-uppgifterna kan i praktiken använda dessa uppgifter i begränsad omfattning eftersom de i princip endast har tillgång till dem för att vidta en specifik åtgärd.

Några tillgångar som föreskrivs i de nya förslagen överensstämmer dock inte med denna logik eftersom syftet med dem faktiskt är att förse myndigheterna med information, men inte att de skall kunna identifiera en person och vidta den åtgärd som förutses i rapporten.

([2]) I juni 2004 sattes en advokat från Portland (USA) i fängelse under två veckor eftersom FBI lyckades matcha hans fingeravtryck med fingeravtryck som påträffats vid terroristbombningen i Madrid (på den plastpåse som innehöll detonatorn). Det visade sig slutligen att det fanns brister i matchningsprocessen, vilket ledde till en feltolkning.

Detta gäller mer specifikt

— tillgång till uppgifter om invandring för asylmyndigheter,

— tillgång till uppgifter om invandring för myndigheter med ansvar för att bevilja flyktingstatus,

— tillgång till rapporter om utlämning, hemlig övervakning och stulna handlingar som skall beslagtas för Europol,

— tillgång till uppgifter om utlämning och lokalisering för Eurojust.

Alla dessa myndigheter kännetecknas av samma sak när det gäller SIS II-uppgifter: de kan inte vidta den specifika åtgärd som avses i definitionen av registreringar.

Tillgång beviljas dem som en källa till information för deras egna syften.

Även mellan dessa myndigheter måste åtskillnad göras mellan dem som har tillgång för sina egna syften, men med ett ganska specifikt syfte, och dem (dvs. Europol och Eurojust) för vilka det inte finns någon specifikation alls av syftet med tillgången. Asylmyndigheter exempelvis har tillgång för ett specifikt syfte, även om det inte är det syfte som avses i registreringen. De kan ha tillgång till uppgifter om invandring ”för att kunna ta ställning till om en asylsökande har uppehållit sig illegalt i en annan medlemsstat”. Men Europol och Eurojust har tillgång till uppgifter i vissa kategorier av registreringar ”vilket är nödvändigt för att de skall kunna utföra sina uppgifter”.

Sammanfattningsvis beviljas tillgång till uppgifter i SIS II i följande tre fall:

— Tillgång för genomförandet av registreringen.

— Tillgång för annat syfte än SIS II, men väl begränsat i förslagen.

— Tillgång för annat syfte än SIS II, men inte exakt beskrivet.

Datatillsynsmannen anser att ju allmännare syftet med tillgång är desto strängare bör de säkerhetsåtgärder som behöver genomföras vara. De allmänna säkerhetsåtgärderna räknas upp i detalj nedan och då kommer Europols och Eurojusts specifika situation att tas upp.

4.2.2 *Villkor för beviljande av tillgång*

1. Tillgång kan under alla omständigheter endast beviljas om det är förenligt med det allmänna syftet med SIS II och överensstämmer med den rättsliga grunden.

   Detta innebär i praktiken att tillgång till uppgifter om invandring enligt förslaget till förordning måste stödja genomförandet av strategier i samband med den rörlighet för personer som ingår i Schengenregelverket.

   På samma sätt skall tillgång till rapporter enligt detta beslut syfta till att underlätta det operativa polissamarbetet och det operativa straffrättsliga samarbetet.

   Datatillsynsmannen pekar i detta sammanhang på kapitlet om tillgång till SIS för enheter som ansvarar för att utfärda registreringsbevis (se punkt 4.6 nedan).

2. Behovet av tillgång till uppgifter i SIS II måste bevisas och att det är omöjligt eller mycket svårt att erhålla uppgifterna på andra, mindre inkräktande sätt. Detta borde ha gjorts i en motivering, och det är som redan nämnts mycket beklagligt att det inte finns någon sådan.

3. Det måste definieras uttryckligen och restriktivt hur uppgifterna kommer att användas.

   Exempelvis har asylmyndigheterna tillgång till uppgifter om invandring ”för att kunna ta ställning till om en asylsökande har uppehållit sig illegalt i en annan medlemsstat”. Men Europol och Eurojust har tillgång till uppgifter i särskilda kategorier av registreringar, ”vilket är nödvändigt för att de skall kunna utföra sina uppgifter”: detta beskrivs inte tillräckligt ingående (se nedan).

4. Villkoren för tillgång måste vara väl definierade och begränsade. Endast de enheter inom dessa organisationer som måste hantera uppgifter i SIS II bör få tillgång till dem. Denna skyldighet enligt artikel 40 i förslaget till beslut och artikel 21.2 i förslaget till förordning bör kompletteras med en skyldighet för de nationella myndigheterna att ha en aktuell förteckning över personer med rätt till tillgång till SIS II. Samma bör gälla för Europol och Eurojust.

5. Det faktum att dessa myndigheter beviljas tillgång till SIS II-uppgifter kan aldrig vara ett skäl till att lägga in eller behålla uppgifter i systemet om de inte är användbara för den specifika registrering som de ingår i. Nya uppgiftskategorier får inte läggas till eftersom de skulle gagna andra informationssystem. I artikel 39 i förslaget till beslut ges till exempel föreskrifter om införande i registreringar av uppgifter om den myndighet som har lagt in registreringen. Dessa uppgifter behövs inte för att vidta en åtgärd (gripande, övervakning, …) och det enda skälet till att de kan införas är förmodligen att de kan gagna Europol eller Eurojust. En tydlig förklaring om behandlingen av dessa uppgifter bör lämnas.

6. Bevarandetiden för uppgifterna får inte förlängas, såvida det inte är nödvändigt med tanke på det ändamål för vilket uppgifterna lades in. Det innebär att även om Europol eller Eurojust har tillgång till dessa uppgifter, är detta inte ett tillräckligt skäl för att behålla dem i systemet (till exempel: när en efterlyst person har utlämnats skall uppgifterna raderas, även om de kan vara till nytta för Europol). Även på denna punkt kommer en noggrann tillsyn att behövas för att säkerställa att de nationella myndigheterna tillämpar detta.

4.2.3 *Tillgång för Europol och Eurojust*

a) *Grunder för tillgång*

Tillgången för Europol och Eurojust till vissa uppgifter i SIS debatterades innan de infördes genom rådets beslut av den 24 februari 2005 ([1]). Bland alla de myndigheter som har tillgång för sina egna syften åtnjuter Europol och Eurojust tillgång som beviljas på ytterst generösa villkor. Fastän användningen av dessa uppgifter beskrivs i kapitel XII i beslutet, är för det första grunderna för att bevilja tillgång inte tillräckligt genomarbetade. Detta är fallet i desto högre grad eftersom Europols och Eurojusts arbetsuppgifter troligen kommer att utvecklas med tiden.

Europeiska datatillsynsmannen uppmanar kommissionen att ge en restriktiv definition av de arbetsuppgifter som berättigar att Europol och Eurojust får tillgång till uppgifter.

b) *Begränsning av uppgifter*

För att undvika att Europol och Eurojust gör ospecificerade eftersökningar och för att förvissa sig om att de endast har tillgång till uppgifter som är nödvändiga för deras arbete, föreslog den gemensamma tillsynsmyndigheten för Schengens informationssystem i sitt yttrande av den 27 september 2005 om förslagen avseende SIS II en begränsning av Europols och Eurojusts tillgång till uppgifter om enskilda vars namn redan förekommer i deras register. Detta skulle garantera att endast de registreringar som är relevanta för dem används. Europeiska datatillsynsmannen stöder denna rekommendation.

c) *Säkerhetsaspekter*

Europeiska datatillsynsmannen välkomnar skyldigheten att föra loggbok över alla transaktioner som utförs av Europol och Eurojust när de är anslutna samt förbudet mot kopiering eller nedladdning av delar av systemet.

Enligt artikel 56 i förslaget till beslut skall det finnas ”en eller två” anslutningspunkter för Europol och Eurojust. Hur förståeligt det än kan vara att en medlemsstat på grund av dess behöriga myndigheters decentraliserade läge behöver mer än en anslutningspunkt, är inte en sådan begäran motiverad på grund av Europols och Eurojusts ställning och verksamhet. Det måste även ur säkerhetssynpunkt understrykas att risken för missbruk ökar genom en mångfald anslutningspunkter, som därför noga bör motiveras med gedignare argument. I avsaknad av övertygande argumentering föreslår därför Europeiska datatillsynsmannen att endast en anslutningspunkt bör beviljas när det gäller Europol och Eurojust.

4.3 **Sammanlänkning av registreringar**

För att upprätta en förbindelse mellan två eller flera registreringar får en medlemsstat enligt artikel 26 i förordningen och artikel 46 i beslutet skapa en länk mellan registreringar i överensstämmelse med nationell lagstiftning.

Fastän länkar mellan registreringar säkert kan vara användbara för kontroller (en arresteringsorder mot en biltjuv kan till exempel länkas till ett stulet fordon), är införandet av länkar mellan registreringar ett mycket typiskt kännetecken för tillvägagångssättet vid en polisutredning.

Sammanlänkning av registreringar kan ha betydande effekter på den berörda personens rättigheter, eftersom personen inte längre bedöms på grundval av uppgifter som endast gäller honom/henne utan på grundval av hans/hennes eventuella anknytning till andra personer. Enskilda om vilka uppgifter är länkade till uppgifter om brottslingar eller efterlysta personer kommer troligen att behandlas med större misstänksamhet än andra. Sammanlänkning av registreringar utgör dessutom en utvidgning av SIS utredningsbefogenheter, eftersom en sammanlänkning kommer att möjliggöra inregistrering av påstådda gäng eller nätverk (om till exempel uppgifter om olagliga invandrare är länkade till uppgifter om människosmugglare). Eftersom upprättandet av länkar regleras genom nationell lagstiftning är slutligen en möjlig konsekvens att länkar som är olagliga i en medlemsstat kan upprättas av en annan medlemsstat, som således matar in ”olagliga” uppgifter i systemet.

([1]) Rådets beslut 2005/211/RIF av den 24 februari 2005 om införande av ett antal nya funktioner för Schengens informationssystem, bland annat i kampen mot terrorism, EUT L 68/44, 15.3.2005.

I rådets slutsatser av den 14 juni 2004 om funktionskraven för SIS II fastställs att varje sammankoppling måste ha ett tydligt driftkrav samt grundas på ett klart fastställt samband och respektera proportionalitetsprincipen. Vidare får inte åtkomsträttigheterna påverkas. Under alla omständigheter måste sammanlänkningen uppfylla kraven i den nationella lagstiftningen för genomförande av direktiv 95/46/EG och/eller konvention nr 108, eftersom sammanlänkningen av registreringar utgör en behandling.

I förslagen upprepas att förekomsten av länkar inte kan ändra tillgångsrättigheterna (annars skulle faktiskt förekomsten av länkar ge tillgång till uppgifter som det inte vore lagligt att behandla enligt nationell lagstiftning, i strid med artikel 6 i direktivet).

Europeiska datatillsynsmannen betonar vikten av en strikt tolkning av artikel 26 i förslaget till förordning och artikel 46 i förslaget till beslut: ett sätt att sörja för detta är att klargöra att myndigheter utan rätt till tillgång till vissa uppgiftskategorier inte får ha tillgång till dessa kategorier och inte ens bör vara medvetna om länkarnas existens. Det måste vara omöjligt att se länkarna om det saknas rättigheter till tillgång till de länkade uppgifterna.

Europeiska datatillsynsmannen skulle vidare vilja rådfrågas om de tekniska åtgärder som säkerställer detta.

4.4 **Registreringar på spärrlista**

4.4.1 *Grunder för införande*

Användningen av ”registreringar om tredjelandsmedborgare i syfte att neka dessa inresa” (artikel 15 i förordningen) har betydande effekter på den enskildes friheter: en enskild person som registrerats enligt denna bestämmelse har inte tillträde till Schengenområdet under flera år. Hittills har detta varit den mest använda registreringen när det gäller antalet registrerade personer. Med tanke på konsekvenserna av denna registrering och antalet berörda personer måste man vara ytterst försiktig vid utformningen och tillämpningen av denna registrering. Detta gäller visserligen även andra registreringar, men Europeiska datatillsynsmannen kommer att ägna ett särskilt kapitel åt denna registrering, eftersom den innebär specifika problem i fråga om grunderna för införande.

Den nya registreringen på spärrlista innebär förbättringar jämfört med den nuvarande situationen, men är inte heller helt tillfredsställande, eftersom den till stor del baserar sig på instrument som ännu inte har antagits eller ens föreslagits.

Förbättringarna består i en tydligare beskrivning av grunderna för införande av uppgifterna. Schengenkonventionens nuvarande lydelse har lett till en situation med betydande skillnader mellan medlemsstaterna i fråga om antalet personer som registrerats enligt artikel 96 i konventionen. Den gemensamma tillsynsmyndigheten för Schengens informationssystem har genomfört en omfattande studie ([1]) om den frågan och kommit med rekommendationer om att ”beslutsfattarna bör överväga att i de olika Schengenstaterna harmonisera skälen till att göra en registrering”.

Lydelsen i den förslagna artikel 15 är mer detaljerad, vilket välkomnas.

Vidare innehåller artikel 15.2 även en förteckning över de fall när personer inte kan registreras eftersom de lagligen vistas på en medlemsstats territorium med tillämpning av olika status. Fastän det skulle kunna härledas från den nuvarande Schengenkonventionen har praxis visat att även tillämpningen av denna mekanism har varierat mellan medlemsstaterna. Förtydligandet är därför ett positivt inslag.

Denna bestämmelse är emellertid även föremål för allvarlig kritik, eftersom den till betydande del baseras på en ännu icke antagen text, nämligen direktivet om återvändande.

Efter antagandet av förslagen om SIS II har kommissionen föreslagit ett ”direktiv om gemensamma normer och förfaranden för återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna” (den 1 september 2005), men så länge som denna text inte är slutlig kan den inte betraktas som en giltig grund för införande av uppgifter i ett system. Det strider bland annat mot artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, eftersom ett intrång i enskildas privatliv skall motiveras med – bland annat – en tydlig och tillgänglig lagstiftning.

Europeiska datatillsynsmannen uppmanar därför kommissionen att antingen ta tillbaka förslaget eller att på grundval av befintlig lagstiftning omarbeta det på så sätt att en enskild person ges möjlighet att veta exakt vilka åtgärder som myndigheterna kan vidta mot honom/henne.

4.4.2 *Tillgång till registreringar enligt artikel 15*

I artikel 18 föreskrivs det vilka myndigheter som har tillgång till dessa registreringar och för vilka ändamål. I artikel 18.1 och 18.2 fastställs det vilka myndigheter som har tillgång till registreringar som lagts in på grundval av direktivet om återvändande. Samma kommentar som ovan gäller.

([1]) Rapport från den gemensamma tillsynsmyndigheten för Schengens informationssystem om en undersökning av användningen av registreringar i Schengens informationssystem enligt artikel 96, Bryssel den 20 juni 2005.

I artikel 18.3 i förslaget förordning beviljas tillgång för myndigheter med ansvar för beviljande av flyktingstatus, enligt ett direktiv som ännu inte ens har föreslagits. Europeiska datatillsynsmannen måste upprepa de ovanstående kommentarerna, eftersom ingen text finns tillgänglig.

4.4.3 *Lagringstid för registreringar enligt artikel 15*

Enligt artikel 20 skall registreringen inte lagras längre än den tid för avvisning som föreskrivs i beslutet (om återsändande eller återvändande). Detta står i överensstämmelse med reglerna om dataskydd. Vidare kommer registreringen att raderas automatiskt efter fem år, såvida inte den medlemsstat som har lagt in uppgifterna i SIS II beslutar om annat.

Lämplig tillsyn på nationell nivå bör garantera att lagringstiden inte automatiskt förlängs utan grund och att medlemsstaterna raderar uppgifterna innan fem år förflutit, om tiden för avvisning råkar vara kortare.

4.5 **Lagringstider**

Principen om lagringstid är oförändrad (som allmän regel skall en registrering raderas från SIS II när den åtgärd som begärts genom registreringen har vidtagits), men förslagen kommer att medföra att lagringstiden för registreringarna allmänt kommer att ha förlängts.

Enligt Schengenkonventionen skulle det senast tre år efter det att uppgifterna lagts in (eller ett år i fråga om uppgifter som lagts in för hemlig övervakning) göras en undersökning av huruvida uppgifterna måste bevaras. I de nya förslagen tänker man sig en automatisk radering (med möjlighet för den medlemsstat som lagt in registreringen att invända) efter fem år i fråga om uppgifter om invandring, tio år i fråga om uppgifter om gripande, försvunna personer och eftersökta eller efterlysta personer som söks för lagföring samt tre år för personer som skall sättas under hemlig övervakning.

Även om medlemsstaterna i princip kommer att vara tvungna att radera uppgifterna när syftet med registreringen är uppfyllt, innebär detta en betydande förlängning av den längsta bevarandetiden (i flertalet fall en trefaldig förlängning) utan någon som helst motivering från kommissionens sida. I fråga om uppgifter om invandring kan man inte annat än våga sig på gissningen att det föreligger ett samband mellan den femåriga bevarandetiden och den varaktighet av förbudet mot inresa som föreslås i utkastet till direktiv om återvändande. I alla övriga fall finns det ingen förklaring som Europeiska datatillsynsmannen känner till.

De potentiella effekterna för dem som registrerats i SIS kan få betydande konsekvenser för de berörda personernas liv. Detta är särskilt oroande när det gäller registreringar av personer för hemlig övervakning eller särskild kontroll, eftersom dessa registreringar kan läggas in på grundval av misstankar.

Europeiska datatillsynsmannen efterlyser en seriös motivering av denna förlängning av lagringstiderna för uppgifter. Om det inte finns någon övertygande motivering föreslår han att lagringstiderna kortas till nuvarande längd och insisterar särskilt på fallet med registreringar för hemlig övervakning eller särskild kontroll.

4.6 **Tillgång för myndigheter med ansvar för att utfärda registreringsbevis för fordon**

Huvudfrågan ligger i valet av en rättslig grund som i högsta grad kan ifrågasättas. Kommissionen anför inget övertygande skäl till att använda en rättslig grund inom första pelaren som avser transporter, för en åtgärd som skulle ge administrativa myndigheter tillgång till SIS för att förebygga och bekämpa brott (olaglig handel med stulna fordon). I punkt 4.2.2 i detta yttrande redogjordes i detalj för nödvändigheten av en stark motivering och en solid rättslig grund för att bevilja tillgång till SIS II.

Europeiska datatillsynsmannen hänvisar till kommentarerna om denna fråga från den gemensamma tillsynsmyndigheten för Schengens informationssystem i dess yttrande om den föreslagna rättsliga grunden för SIS II. I synnerhet skall man följa förslaget från den gemensamma tillsynsmyndigheten för Schengens informationssystem om att ändra förslaget till beslut så att denna tillgång omfattas.

5. KOMMISSIONENS OCH MEDLEMSSTATERNAS ROLL

En tydlig beskrivning och fördelning av ansvarsområdena när det gäller SIS II är av största vikt inte bara för att systemet skall fungera smidigt utan även ur tillsynssynpunkt. Fördelningen av tillsynsbefogenheter kommer att vara en följd av beskrivningen av ansvarsområdena, och fullständig tydlighet är därför nödvändig.

5.1 **Kommissionens roll**

Europeiska datatillsynsmannen välkomnar kapitel III i båda förslagen, vilket beskriver kommissionens roll och ansvar när det gäller SIS II (som en ”operativ förvaltningsroll”). Ett sådant klarläggande fanns inte i förslaget om VIS. Kommissionens roll definieras emellertid inte uttömmande i endast det kapitlet. Såsom diskuteras i kapitel 9 i detta yttrande är kommissionen även engagerad i genomförandet och förvaltningen av systemet genom kommittéförfarandet.

I fråga om dataskydd har kommissionen en roll som redan erkänns i VIS- och Eurodac-systemen, nämligen att ansvara för operativ förvaltning. Tillsammans med dess mer betydande roll att utveckla och underhålla systemet bör detta betraktas som rollen för en registeransvarig *sui generis*. Såsom redan nämnts i Europeiska datatillsynsmannens yttrande om VIS är rollen mycket mer omfattande än registerförarens roll, men även mer begränsad än en normal registeransvarigs roll, eftersom kommissionen inte har tillgång till de uppgifter som behandlas i SIS II.

Eftersom SIS II kommer att bygga på komplexa system, varav en del är beroende av ny teknik, insisterar Europeiska datatillsynsmannen på en förstärkning av kommissionens ansvar för att hålla systemen fullt moderna genom att införa bästa tillgängliga teknik för säkerhet och dataskydd.

Det bör därför tilläggas i artikel 12 i förslagen att kommissionen regelbundet skall föreslå införandet av ny teknik som utgör den modernaste på detta område och kommer att höja nivån på dataskyddet och säkerheten samt underlätta arbetet för de nationella myndigheter som har tillgång till dessa uppgifter.

5.2 **Medlemsstaternas roll**

Medlemsstaternas situation är inte helt klar, eftersom det är svårt att veta vilken myndighet (vilka myndigheter) som kommer att vara registeransvarig(a).

I förslagen beskrivs en roll för nationella SIS II-byrån (för att säkerställa att de behöriga myndigheterna har tillgång till SIS II) och för Sirenemyndigheterna (för att säkerställa utbyte av all tilläggsinformation). En medlemsstat skall också säkerställa funktionen och säkerheten hos sitt NS (nationella system). Det står inte klart huruvida någon av de ovannämnda myndigheterna skall ansvara för detta sista ansvarsområde. Under alla omständigheter behövs ett förtydligande i detta avseende.

När det gäller dataskydd bör kommissionen och medlemsstaterna betraktas som gemensamt registeransvariga, var och en med specifika ansvarsområden. Erkännandet av dessa uppdrag som kompletterar varandra är det enda sättet att inte lämna något område av verksamheten inom SIS II utan tillsyn.

6. **REGISTRERADES RÄTTIGHETER**

6.1 **Information**

6.1.1 *Förslaget till förordning*

I artikel 28 i förslaget till förordning anges den registrerades rätt till information, och man följer i huvudsak artikel 10 i direktiv 95/46. Detta är en välkommen förändring jämfört med den nuvarande situationen, där det inte explicit anges någon rätt till information i konventionen. Det finns emellertid visst utrymme för förbättringar på följande punkter.

Viss information bör läggas till i förteckningen, eftersom detta skulle bidra till att garantera en rättvis behandling av den registrerade ([1]). Denna information bör avse lagringstiden för uppgifterna, rätten att begära omprövning eller överklagande av beslutet om inläggning av en registrering (i vissa fall; se artikel 15.3 i förslaget till förordning), möjligheten att få hjälp av dataskyddsmyndigheten samt rättsmedel.

I förslaget till förordning finns det ingen hänvisning till den tidpunkt då informationen skall lämnas. Detta kan göra det omöjligt för den registrerade att göra sina rättigheter gällande. För att dessa rättigheter skall bli faktiska, bör förordningen ange en exakt tidpunkt då information skall lämnas, beroende på vilken myndighet som har lagt in registreringen.

Det vore för det första en praktisk lösning att lägga till information om registreringen i det beslut som registreringen grundar sig på: antingen ett rättsligt eller administrativt beslut grundat på ett hot mot allmän ordning (…) eller ett beslut om återvändande eller utvisning tillsammans med ett återreseförbud. Detta bör läggas till i artikel 28 i förordningen.

6.1.2 *Förslaget till beslut*

I artikel 50 i beslutet föreskrivs att information skall utlämnas på begäran av den registrerade personen och där anges också de möjliga skälen för att vägra utlämnande av denna information. Begränsningarna av denna rättighet är naturligtvis förståeliga med hänsyn till uppgifternas art och det sammanhang i vilket de behandlas.

Rätten till information bör emellertid inte vara avhängigt av en ansökan från den registrerade personen (detta skulle faktiskt snarare vara definitionen av en ansökan om tillgång). Det kan förmodas att behovet av att ”ansöka om” information motiverades av de fall då den registrerade personen inte kan informeras därför att han inte är lokaliserad.

En bättre lösning på problemet skulle vara att lägga till ett undantag till rätten till information i de fall då det visar sig omöjligt eller medför en oproportionerlig ansträngning att lämna ut information. Artikel 50 i beslutet bör ändras i enlighet härmed.

([1]) Se yttrandet från Europeiska datatillsynsmannen om inrätttandet av informationssystemet för viseringar, punkt 3.10.1 med samma innebörd.

Denna lösning skulle också vara förenlig med tillämpningen av utkastet till rambeslut om uppgiftsskydd i tredje pelaren.

6.2 **Tillgång**

I både förslaget till förordning och förslaget till beslut föreskrivs tidsfrister för besvarande av ansökningar om tillgång, vilket är en positiv utveckling. Eftersom förfarandet för utövandet av rätten till tillgång fastställs på nationell nivå kan man emellertid undra hur de tidsfrister som föreskrivs i förslagen kan samverka med de befintliga förfarandena, i synnerhet om medlemsstaterna har kortare tidsfrister för att besvara en ansökan om tillgång. Det bör klargöras att de tidsfrister som är mest förmånliga för den registrerade personen bör tillämpas.

6.2.1 *Förslaget till förordning*

Det är värt att notera att de begränsningar av rätten till tillgång (”skall avslås, om det kan skada verkställigheten av rättsliga uppdrag som rapporten avser, eller om någon annan persons rätt och frihet måste skyddas”) som för närvarande finns i Schengenkonventionen inte förekommer i förslaget till förordning.

Emellertid beror detta förmodligen på tillämpligheten av direktiv 95/46/EG, där det föreskrivs (i artikel 13) att det finns möjlighet att införa undantag i nationella lagstiftningar. I varje fall bör det påpekas att användningen av artikel 13 i nationell lagstiftning för att begränsa rätten till tillgång alltid bör vara förenlig med artikel 8 i ECHR och att detta endast bör ske i begränsade fall.

6.2.2 *Förslaget till beslut*

I förslaget till beslut begränsas rätten till tillgång på samma sätt som i Schengenkonventionen. Förslaget till rambeslut innehåller i sak samma begränsningar av rätten till tillgång och därför bör antagandet av detta instrument inte innebära någon betydande skillnad härvidlag.

Eftersom tillgången till uppgifter med anknytning till brottsbekämpning i flera medlemsstater är ”indirekt” (det vill säga utövas via den nationella myndigheten med ansvar för uppgiftsskydd) torde det vara lämpligt att föreskriva en skyldighet för myndigheter med ansvar för uppgiftsskydd att samarbeta aktivt i utövandet av rätten till tillgång.

6.3 **Rätt till omprövning eller överklagande av ett beslut om att lägga in en registrering**

Enligt artikel 15.3 i förordningen har en registrerad person rätt att få ett beslut om att lägga in en registrering omprövat av eller att överklaga till en rättslig myndighet, om beslutet fattas av en administrativ myndighet. Detta är ett välkommet tillägg jämfört med den nuvarande Schengenkonventionen.

Detta understryker behovet av att den registrerade personen erhåller fullständig information och att det sker i tid, såsom nämndes i punkt 6.1 ovan: utan denna rättighet förblir denna nya rättighet teoretisk.

6.4 **Rättsmedel**

I artikel 30 i förslaget till förordning och artikel 52 i förslaget till beslut föreskrivs rätten att väcka talan eller klagomål inför domstol i vilken medlemsstat som helst om den registrerade personen vägras rätten att ta del av eller att rätta eller radera uppgifter eller rätten att få information eller upprättelse.

Lydelsen (”varje individ som befinner sig på någon av medlemsstaternas territorium”) antyder att den klagande måste befinna sig fysiskt på territoriet för att väcka sin talan inför domstol. Denna territoriella begränsning motiveras inte och kan göra rätten till rättsmedel ineffektiv, eftersom den klagande mycket ofta väcker talan just därför att han inte beviljas tillträde till Schengenterritoriet. När det gäller förslaget till förordning måste dessutom artikel 22 i direktivet beaktas eftersom direktivet är *lex generalis*; enligt denna artikel har ”var och en” rätt till ett rättsmedel, oberoende av bostadsort. Förslaget till rambeslut innehåller inte heller någon territoriell begränsning. Datatillsynsmannen föreslår att den territoriella begränsningen i artikel 30 och artikel 52 stryks.

7. **TILLSYN**

7.1 **Inledande anmärkning: ansvarsfördelning**

Enligt förslagen skall tillsynsuppgiften fördelas mellan nationella tillsynsmyndigheter ([1]) och datatillsynsmannen, var och en för sitt ansvarsområde. Detta är i överensstämmelse med förslagens syn på tillämplig lagstiftning och ansvar för driften och användningen av SIS II och med behovet av en effektiv tillsyn.

Datatillsynsmannen välkomnar därför detta synsätt i artikel 31 i förslaget till förordning och artikel 53 i förslaget till beslut. För att göra respektive uppgifter tydligare och mer begripliga föreslår datatillsynsmannen dock att varje artikel skall delas upp i flera bestämmelser och att var och en av dessa skall ägnas åt en tillsynsnivå, på samma sätt som i förslagen om VIS.

([1]) Tillsynsmyndigheterna för Europol och Eurojust är också involverade men i mindre utsträckning.

7.2 **Tillsyn från nationella myndigheter med ansvar för uppgiftsskydd**

Enligt artikel 31 i förslaget till förordning och artikel 53 i förslaget till beslut skall varje medlemsstat se till att en oberoende myndighet övervakar att behandlingen av personuppgifter i SIS II sker enligt gällande regler.

Artikel 53 i förslaget till beslut innehåller ett tillägg om att enskilda individer skall ha rätt att begära att tillsynsmyndigheten kontrollerar att hans eller hennes personuppgifter behandlas enligt gällande regler. Någon liknande bestämmelse finns inte i förslaget till förordning eftersom direktivet är tillämpligt som *lex generalis*. Därför måste det anses att nationella myndigheter med ansvar för uppgiftsskydd kan utöva, med avseende på SIS II, alla de befogenheter som den tilldelas genom artikel 28 i direktiv 95/46/EG, inklusive kontroll av om behandlingen av uppgifter är enligt gällande regler. I artikel 31.1 i förordningen klargörs deras uppgift, men detta kan inte innebära en begränsning av dessa befogenheter. Erkännandet av dessa befogenheter bör klargöras i förslaget till förordning.

När det gäller förslaget till beslut tillerkänns de nationella tillsynsmyndigheterna mer omfattande skyldigheter genom detta eftersom dess *lex generalis* är annorlunda. En situation då tillsynsmyndigheter skulle ha olika uppdrag och befogenheter beroende på vilken kategori av uppgifter som behandlas är emellertid inte sund och mycket svårhanterlig i praktiken. Därför bör den undvikas antingen genom att dessa myndigheter tillerkänns samma befogenheter i själva förslaget till beslut eller genom att det hänvisas till en annan *lex generalis* (nämligen rambeslutet om uppgiftsskydd i tredje pelaren) varigenom de myndigheter som ansvarar för uppgiftsskydd tilldelas fler befogenheter.

7.3 **Tillsyn från datatillsynsmannen**

Datatillsynsmannen övervakar att den behandling av uppgifter som bedrivs av kommissionen utförs i enlighet med förslagen. På samma sätt bör datatillsynsmannen kunna utöva alla sina befogenheter enligt förordning 45/2001, dock med hänsyn till kommissionens begränsade befogenheter med avseende på själva uppgifterna.

Det bör tilläggas att datatillsynsmannen enligt artikel 46 f i förordning nr 45/2001 skall ”samarbeta med de nationella tillsynsmyndigheter … i den omfattning som behövs för att de skall kunna fullgöra sina respektive uppgifter”. Samarbetet med medlemsstaterna vid tillsynen av SIS II härrör inte endast från förslagen utan även från förordning 45/2001.

7.4 **Gemensam tillsyn**

I förslagen erkänns också behovet av att samordna de olika, berörda myndigheternas tillsynsverksamhet. Enligt artikel 31 i förslaget till förordning och artikel 53 i förslaget till beslut ska ”de nationella tillsynsmyndigheterna och Europeiska datatillsynsmannen … samarbeta aktivt. Europeiska datatillsynsmannen skall för detta ändamål sammankalla ett möte minst en gång om året.”

Tillsynsmannen välkomnar detta förslag som i sak innehåller de nödvändiga faktorerna för att upprätta samarbetet – vilket verkligen är mycket väsentligt – mellan de myndigheter som ansvarar för tillsyn på nationell och europeisk nivå. Det bör understrykas att det i förslagen föreskrivs ett möte minst en gång om året men att detta skall betraktas som ett minimum.

När det gäller dessa bestämmelser (artikel 31 i förslaget till förordning och artikel 53 i förslaget till beslut) kunde det emellertid vara lämpligt med vissa klargöranden om innehållet i denna samordning. Den nuvarande gemensamma tillsynsmyndigheten har befogenhet att granska svårigheter med tolkning eller tillämpning av konventionen, att studera problem som kan förekomma när det gäller utövandet av oberoende tillsyn eller rätten till tillgång samt att utforma harmoniserade förslag till gemensamma lösningar på befintliga problem.

De nya förslagen kan inte leda till en urvattning av den nuvarande omfattningen av den gemensamma tillsynen. Om det är uppenbart att myndigheter med ansvar för uppgiftsskydd med avseende på SIS II han utöva alla de tillsynsbefogenheter som de tilldelas genom direktivet, kan samarbetet mellan dessa myndigheter omfatta breda aspekter av tillsynen av SIS II, inklusive den befintliga gemensamma tillsynsmyndighetens arbetsuppgifter enligt artikel 155 i Schengenkonventionen.

För att klargöra detta helt och hållet skulle det vara lämpligt att bekräfta detta uttryckligen i förslagen.

8. **SÄKERHET**

Förvaltningen av och respekten för en optimal säkerhetsnivå för SIS II utgör ett grundläggande krav för säkerställande av ett adekvat skydd av personuppgifter som lagras i databasen. För att erhålla denna tillfredställande skyddsnivå måste lämpliga säkerhetsgarantier införas när det gäller hanteringen av potentiella risker för systemets infrastruktur och för de berörda personerna. Detta ämne diskuteras nu i olika delar av förslaget och därvidlag krävs det en viss förbättring.

Artiklarna 10 och 13 i förslaget innehåller olika åtgärder för uppgiftssäkerhet och där anges också vilka typer av missbruk som behöver förebyggas. Datatillsynsmannen välkomnar att bestämmelser om systematisk (egen)kontroll av säkerhetsåtgärder ingår i dessa artiklar.

Artikel 59 i förslaget till beslut och artikel 34 i förslaget till förordning, som handlar om övervakning och utvärdering, bör emellertid inte endast röra aspekterna produktivitet, kostnadseffektivitet och tjänsternas kvalitet utan även överensstämmelsen med rättsliga krav, i synnerhet inom området uppgiftsskydd. Datatillsynsmannen rekommenderar därför att räckvidden för dessa artiklar utvidgas till övervakning av och rapportering om huruvida behandlingen sker enligt gällande regler.

Som komplement till artikel 10.1 f eller artikel 18 i förslaget till beslut och artikel 17 i förslaget till förordning beträffande den vederbörligen auktoriserade personal som har tillgång till uppgifterna bör det tilläggas att medlemsstaterna (liksom Europol och Eurojust) bör se till att exakta användarprofiler är tillgängliga (vilka bör stå till de nationella tillsynsmyndigheternas förfogande för kontroller). Utöver dessa användarprofiler måste en fullständig förteckning över användaridentiteter utarbetas och kontinuerligt uppdateras av medlemsstaterna. Detta gäller även kommissionen i tillämpliga delar.

Dessa säkerhetsåtgärder kompletteras med skyddsåtgärder med avseende på övervakning och organisation. I artikel 14 i förslagen beskrivs villkoren för och syftena med registreringarna av alla databehandlingsoperationerna. Dessa registreringar skall inte bara lagras för övervakning av uppgiftsskyddet och säkerställande av uppgiftssäkerheten utan även för konsolidering av den regelbundna egenkontrollen av SIS II, såsom föreskrivs i artikel 10. Egenkontrollrapporterna kommer att bidra till att tillsynsmyndigheterna utför sina arbetsuppgifter effektivt och att dessa kan fastställa de svagaste punkterna och koncentrera sig på dem under sitt egenkontrollförfarande.

Såsom nämndes tidigare i detta yttrande måste en ökning av antalet anslutningspunkter till systemet motiveras noggrant eftersom det automatiskt ökar riskerna för missbruk. I artikel 4.1 b 9 i förslagen bör det därför konkret påvisas att det behövs en andra anslutningspunkt.

Förslagen innehåller ingen tydlig förklaring av behovet av nationella kopior av det centrala systemet och föranleder allvarliga farhågor om den övergripande risk- och säkerhetsnivån för systemet, till exempel följande:

— En ökning av antalet kopior ökar riskerna för missbruk (särskilt med tanke på förekomsten av nya uppgifter, till exempel biometriska uppgifter).

— De uppgifter som behandlas i dessa kopior är inte väl definierade.

— Kraven på korrekthet, kvalitet och tillgänglighet i artikel 9 medför stora tekniska utmaningar och ökar därför kostnaden i enlighet med den senaste tillgängliga tekniken.

— De nationella myndigheternas tillsyn av dessa kopior kommer att kräva ytterligare mänskliga och finansiella resurser, vilka kanske inte alltid kommer att stå till förfogande.

Med hänsyn till de risker som det innebär är datatillsynsmannen inte övertygad om vare sig behovet (med tanke på tillgänglig teknik) eller mervärdet av användningen av nationella kopior. Han rekommenderar att möjligheten för medlemsstaterna att använda nationella kopior skall strykas.

Om nationella kopior skall tas fram, erinrar datatillsynsmannen dock om att en strikt princip om begränsning rörande syftet måste tillämpas på den nationella användningen av dem. Likaså får man aldrig söka i den nationella kopian på andra sätt än i den centrala databasen.

Lagligheten när det gäller behandlingen av personuppgifter grundas på fullständig respekt för uppgiftssäkerhet och uppgiftsintegritet. Datatillsynsmannen kommer att på ett effektivt sätt övervaka dessa processer, om han inte endast kan övervaka uppgiftssäkerheten utan även uppgifternas integritet genom analys av de tillgängliga loggböckerna. Det är därför nödvändigt att lägga till ”uppgifternas integritet” i artikel 14.6.

9. **KOMMITTÉFÖRFARANDE**

I förslagen föreskrivs kommittéförfaranden i flera fall där det krävs tekniska beslut för genomförandet eller förvaltningen av SIS II. Såsom angavs i yttrandet om VIS av liknande skäl kommer dessa beslut att få betydande konsekvenser för det korrekta genomförandet av principen om syfte och proportionalitet.

Datatillsynsmannen rekommenderar att beslut med väsentliga konsekvenser för uppgiftsskyddet, till exempel tillgång till och införande av uppgifter, utbyte av kompletterande information, uppgifternas kvalitet och kompatibilitet mellan rapporter, nationella kopiors tekniska överensstämmelse osv., bör antas genom en förordning eller ett beslut och helst med hjälp av medbeslutandeförfarandet ([1]).

([1]) Se i detta sammanhang datatillsynsmannens yttrande om Informationssystemet för viseringar, punkt 3.12, och datatillsynsmannens yttrande om förslaget till direktiv om lagring av uppgifter som behandlats i samband med tillhandhållande av allmänt tillgängliga elektroniska kommunikationstjänster, vilket utfärdades den 26 september 2005, punkt 60.

När det gäller alla andra fall med konsekvenser för uppgiftsskyddet bör datatillsynsmannen ges möjlighet att ge rekommendation om de val som dessa kommittéer gör.

Datatillsynsmannens rådgivande roll bör anges i artiklarna 60 och 61 i beslutet och artikel 35 i förordningen.

I det mer specifika fallet rörande tekniska bestämmelser för sammanlänkade registreringar (artikel 26 i förordningen och artikel 46 i beslutet) måste behovet av olika kommittéförfaranden (rådgivande kommittéförfarande för beslutet och föreskrivande kommittéförfarande för förordningen) förklaras.

10. **INTEROPERABILITET**

Eftersom kommissionens meddelande om interoperabiliteten för framtida system inom EU ännu inte föreligger, är det svårt att på ett korrekt sätt utvärdera mervärdet av den planerade men ännu inte definierade samverkan.

I detta sammanhang vill datatillsynsmannen också hänvisa till rådets uttalande av den 25 mars 2004 om bekämpande av terrorism, där kommissionen uppmanas att lägga fram förslag i syfte att öka interoperabilitet och samverkan mellan informationssystem (SIS, VIS och Eurodac). Han vill också hänvisa till den pågående diskussionen om vilket organ som skall anförtros förvaltningen av de olika storskaliga systemen i framtiden (se även punkt 3.8 i detta yttrande).

Datatillsynsmannen meddelade redan i yttrandet om informationssystemet för viseringar att interoperabilitet är en viktig och avgörande förutsättning för att storskaliga IT-system som SIS II skall bli effektiva. 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 behålla en hög säkerhetsnivå på ett område utan inre gränskontroller mellan medlemsstaterna 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; den rapport som sänds från en medlemsstats myndigheter måste vara interoperabel med sådana som översänts av alla andra medlemsstaters myndigheter.

  — 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 till eller användning av vissa uppgifter kan erhålla dessa via ett annat informationssystem. I den mån man kan upptäcka det genom att läsa förslagen tycks det till exempel som om ett automatiskt fingeravtrycksidentifieringssystem (AFIS) inte kommer att finnas under SIS II:s första år; det görs endast en hänvisning till en kommande biometrisk sökmotor. Om ett scenario planeras där AFIS från andra EU-system används, bör det dokumenteras tydligt med de nödvändiga skyddsåtgärder som krävs för sådana synergier.

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

11. **SAMMANFATTNING AV SLUTSATSER**

11.1 **Allmänna punkter**

1. Datatillsynsmannen välkomnar flera positiva aspekter av förslagen, som på en del punkter innebär en förbättring jämfört med den situation som nu råder. Han konstaterar att bestämmelserna om uppgiftsskydd generellt sett har utarbetats med stor omsorg.

2. Datatillsynsmannen framhåller att den nya rättsliga ordningen, även om den är komplex, bör

   — garantera en hög nivå på uppgiftsskyddet,

   — vara förutsägbar för medborgarna och för de myndigheter som utbyter uppgifter,

   — vara konsekvent i sin tillämpning på olika kontexter (första eller tredje pelaren).

3. Tillägget av nya element i SIS II, vilket ökar dess eventuella inverkan på enskilda människors liv, bör dessutom följas av strängare säkerhetsåtgärder vilka beskrivs i yttrandet. Följande kan särskilt framföras:

— Tillgång till uppgifter i SIS II får inte ges till nya myndigheter om det inte finns en mycket stark motivering för detta. Den bör även begränsas så mycket som möjligt, när det gäller både tillgängliga uppgifter och bemyndigade personer.

— Sammankoppling av registreringar får aldrig, ens indirekt, leda till en ändring av rätten till tillgång.

— Icke antagen lagstiftning får inte betraktas som en giltig grund för införande av uppgifter i SIS II (registreringar för att vägra inresa).

— Den rättsliga grunden för tillgång för myndigheter som ansvarar för utfärdande av registreringsbevis för fordon bör övervägas på nytt eftersom den huvudsakligen är avsedd att bekämpa brottslighet.

— Datatillsynsmannen inser att användningen av biometeriska uppgifter kan förbättra systemets resultat och hjälpa offren för identitetsstöld. Effekten av detta införande verkar dock inte vara tillräckligt genomtänkt och dessa uppgifters tillförlitlighet förefaller överskattad.

11.2 **Särskilda påpekanden**

1. Datatillsynsmannen välkomnar kommissionens erkännande att förordning nr 45/2001 gäller all behandling av uppgifter av kommissionen i SIS II, eftersom den kommer att bidra till att garantera en enhetlig och homogen tillämpning av reglerna för skydd av enskilda personers grundläggande rättigheter och friheter när det gäller behandlingen av personuppgifter.

2. För att säkerställa en strikt begränsning av syftet på nationell nivå rekommenderar datatillsynsmannen att det i SIS II-förslagen (dvs. artikel 21 i förslaget till förordning och artikel 40 i förslaget till beslut) införs en bestämmelse med samma verkan som den nuvarande artikel 102.4 i Schengenkonventionen, varigenom medlemsstaternas möjlighet att bestämma om annan användning av uppgifterna än den som förutses i SIS II-texterna begränsas.

3. Följande stränga villkor bör gälla när en myndighet beviljas tillgång till SIS II-uppgifter:

— Tillgången måste vara förenlig med SIS II:s allmänna syfte och överensstämma med dess rättsliga grund.

— Behovet av tillgång till SIS II-uppgifter måste bevisas.

— Det måste uttryckligen och restriktivt preciseras hur uppgifterna kommer att användas.

— Villkoren för tillgång måste vara väl definierade och begränsade. I synnerhet bör det finnas en aktuell förteckning över personer med rätt till tillgång till SIS II även för Europol och Eurojust.

— Det faktum att dessa myndigheter beviljas tillgång till SIS II-uppgifter kan aldrig vara ett skäl till att införa eller behålla uppgifter i systemet om de inte är användbara för den särskilda registrering som de ingår i.

— Bevarandetiden för uppgifter får inte förlängas om det inte är nödvändigt för det syfte för vilket uppgifterna infördes.

4. I de specifika fallen Europol och Eurojust uppmanar datatillsynsmannen kommissionen att på ett restriktivt sätt precisera de uppgifter där tillgång är motiverad för att de skall kunna utföras. Europols och Eurojusts tillgång bör dessutom begränsas till uppgifter om enskilda personer vars namn redan förekommer i deras filer. Det föreslås också att Europol och Eurojust beviljas endast en anslutningspunkt.

5. När det gäller registreringar i syfte att vägra inresa bör de bestämmelser som grundar sig på ännu inte antagen lagstiftning antingen dras tillbaka eller formuleras om på ett sätt – baserat på befintlig lagstiftning – som låter de enskilda personerna få veta exakt vilka åtgärder myndigheterna kan vidta beträffande dem.

6. Bevarandetiderna för uppgifter har förlängts utan att någon riktig motivering till detta har lämnats. Om det inte finns någon övertygande motivering bör de återgå till sin nuvarande längd, särskilt när det gäller registreringar för hemlig övervakning eller särskilda kontroller.

7. Kommissionens roll beskrivs som den roll som en ansvarig för operativ förvaltning har. I kombination med dess huvudroll i utvecklingen och underhållet av systemet bör detta ses som den roll som en registeransvarig *sui generis* har. Den är mycket större än en registerförares roll, men är också mer begränsad än en vanlig registeransvarigs roll, eftersom kommissionen inte har någon tillgång till de uppgifter som behandlas i SIS II.

   I enlighet med den rollen bör det tilläggas i artikel 12 i båda förslagen att kommissionen regelbundet bör föreslå genomförandet av nya tekniker som ger en bild av det aktuella forskningsläget på detta område och som kommer att öka uppgiftsskyddet och säkerheten.

8. När det gäller medlemsstaternas roll behövs ett klargörande i fråga om myndigheter som är registeransvariga.

9. Beträffande informationen om den registrerade gäller följande:

   — I förslaget till förordning bör viss information läggas till på förteckningen, nämligen bevarandetiden för uppgifterna, förekomsten av rättigheten att begära en översyn eller överklagan av beslutet att utfärda en registrering, möjligheten att få stöd från dataskyddsmyndigheten och förekomsten av rättsmedel.

     När det gäller den tidpunkt då denna information lämnas bör det dessutom finnas en skyldighet att lämna information om registreringen i det beslut som först och främst utgör grunden för registreringen.

   — I förslaget till beslut bör artikel 50 ändras så att rätten till information inte är beroende av en begäran från den registrerade.

10. Vad gäller tidsfristerna för besvarandet av en begäran om tillgång välkomnas att sådana införs i beslutet. Om tidsfrister införs även i nationell lagstiftning bör det klargöras att de tidsfrister som är mest fördelaktiga för den registrerade bör tillämpas.

    Det kan dessutom vara lämpligt att föreskriva en skyldighet för dataskyddsmyndigheterna att samarbeta aktivt vid utövandet av rätten till tillgång.

11. Vad beträffar rätten till rättsmedel föreslår datatillsynsmannen att den territoriella begränsningen i artiklarna 30 och 52 stryks.

12. När det gäller de nationella dataskyddsmyndigheternas befogenheter kan följande framföras:

    — I förordningen måste det beaktas att de i fråga om SIS II kan utöva alla de befogenheter som tilldelas dem genom artikel 28 i direktiv 95/46/EG, och detta bör klargöras i förslaget till förordning.

    — I förslaget till beslut bör tillsynsmyndigheterna tillerkännas samma befogenheter som i förordningen/direktivet.

13. Vad beträffar datatillsynsmannens befogenheter bör denne kunna utöva alla sina befogenheter enligt förordning nr 45/2001, dock med beaktande av kommissionens begränsade befogenheter när det gäller själva uppgifterna.

14. Beträffande samordnad övervakning erkänns i förslagen även behovet av att samordna de olika inblandade myndigheternas tillsynsverksamheter. Datatillsynsmannen välkomnar att de i huvudsak innehåller de nödvändiga inslagen för att skapa samarbete mellan de myndigheter som ansvarar för tillsynen på nationell och europeisk nivå. Dessa bestämmelser (artikel 31 i förslaget till förordning och artikel 53 i förslaget till beslut) skulle dock behöva en del klargöranden av innehållet i den samordningen.

15. Artiklarna 10 och 13 i förslaget innehåller olika åtgärder för datasäkerhet och införandet av bestämmelser om systematisk (egen)kontroll av säkerhetsåtgärder välkomnas.

    — Artikel 59 i förslaget till beslut och artikel 34 i förslaget till förordning som innehåller bestämmelser om övervakning och utvärdering bör dock inte endast gälla aspekterna produktivitet, kostnadseffektivitet och tjänsternas kvalitet utan även efterlevnad av rättsliga krav, särskilt på området uppgiftsskydd. Dessa bestämmelser bör ändras i enlighet därmed.

    — Som ett komplement till artikel 10.1 f eller artikel 18 i förslaget till beslut och artikel 17 i förslaget till förordning bör det dessutom läggas till att medlemsstaterna, Europol och Eurojust bör se till att exakta användarprofiler finns tillgängliga (dessa bör ställas till förfogande för de nationella tillsynsmyndigheterna för kontroll). Förutom dessa användarprofiler måste en fullständig förteckning över användaridentiteterna göras och hållas ständigt aktuell av medlemsstaterna. Samma sak gäller kommissionen.

    — Lagenligheten i behandlingen av personuppgifter bygger på den strikta respekten av uppgifternas säkerhet och integritet. Datatillsynsmannen bör ha möjlighet att övervaka inte bara uppgifternas säkerhet utan även uppgifternas integritet genom en analys av tillgängliga loggar. Det är således nödvändigt att lägga till ”uppgifternas integritet” i artikel 14.6.

16. Användningen av nationella kopior kan medföra många extra risker. Datatillsynsmannen är varken övertygad om behovet (med hänsyn till tillgängliga tekniker) eller mervärdet av användningen av nationella kopior. Han rekommenderar att man undviker eller åtminstone allvarligt begränsar medlemsstaternas möjlighet att använda nationella kopior. Om nationella kopior skall tas fram måste dock en princip om strikt begränsning av syftet tillämpas på deras nationella användning. Likaledes får man aldrig söka i en nationell kopia på annat sätt än i den centrala databasen.

17. När det gäller kommittéförfarandet bör beslut med betydande konsekvenser för uppgiftsskydd fattas genom en förordning eller ett beslut, helst genom ett medbeslutandeförfarande. Om kommittéförfarandet tillämpas bör datatillsynsmannens rådgivande roll tas med i artiklarna 60 och 61 i beslutet och artikel 35 i förordningen.

18. Systemens interoperabilitet får inte genomföras i strid med principen om begränsning av syftet och alla förslag i denna fråga bör föreläggas datatillsynsmannen.

Utfärdat i Bryssel den 19 oktober 2005

Peter HUSTINX

Europeisk datatillsynsmannen