DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE

Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse

— om forslaget til Rådets afgørelse om oprettelse, drift og brug af anden generation af Schengen-informationssystemet (SIS II) (KOM(2005) 230 endelig)

— om forslaget til Europa-Parlamentets og Rådets forordning om oprettelse, drift og brug af anden generation af Schengen-informationssystemet (SIS II) (KOM(2005) 236 endelig)

— om forslaget til Europa-Parlamentets og Rådets forordning om adgang til anden generation af Schengen-informationssystemet (SIS II) for de tjenester i medlemsstaterne, der har ansvaret for udstedelse af registreringsattester for motorkøretøjer (KOM(2005) 237 endelig)

(2006/C 91/11)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE,

som henviser til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 286,

som henviser til Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 8,

som henviser til Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger,

som henviser til Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger, særlig artikel 41, og

som henviser til Kommissionens anmodning om udtalelse, jf. artikel 28, stk. 2, i forordning (EF) nr. 45/2001, modtaget den 17. juni 2005,

HAR VEDTAGET FØLGENDE UDTALELSE:

1. INDLEDNING

1.1. Baggrund

Schengen-informationssystemet (SIS) er et omfattende it-system i EU, der er indført som en kompensationsforanstaltning efter afskaffelsen af kontrollen ved de indre grænser inden for Schengen-området. SIS gør det muligt for medlemsstaternes kompetente myndigheder at udveksle oplysninger, der anvendes ved kontrol af personer og genstande ved de ydre grænser eller på medlemsstaternes territorier samt ved udstedelse af visa og opholdstilladelser.

Schengen-konventionen, der var en regeringsaftale, trådte i kraft i 1995. SIS, som er en del af Schengen-konventionen, blev senere integreret i EU-rammerne ved Amsterdam-traktaten.

En ny »anden generation« af Schengen-informationssystemet (SIS II) vil erstatte det nuværende system, således at Schengen-området kan udvides til de nye medlemsstater. SIS II vil også indføre nye funktioner i systemet. De Schengen-bestemmelser, der er udarbejdet inden for rammerne af regeringskonferencer, vil blive fuldt omdannet til klassiske instrumenter i EU-retten.

Den 1. juni 2005 forelagde Europa-Kommissionen tre forslag om indførelse af SIS II. Der er tale om:

— et forslag til forordning baseret på afsnit IV i EF-traktaten (visum-, asyl-, indvandrings- og andre politikker vedrørende personers frie bevægelighed), som omfatter SIS II-aspekterne under første søjle (indvandring), i det følgende benævnt »den foreslåede forordning«

— et forslag til afgørelse baseret på afsnit VI i EU-traktaten (politimæssigt og retligt samarbejde i straffesager), som omfatter SIS's anvendelse til formål under tredje søjle, i det følgende benævnt »den foreslåede afgørelse«

— et forslag til forordning baseret på afsnit V (transport) om især adgangen til SIS-data for de myndigheder, der har ansvaret for køretøjsregistrering; dette forslag behandles særskilt (jf. punkt 4.6).

Det skal i denne forbindelse nævnes, at Kommissionen i løbet af de kommende måneder vil udsende en meddelelse om interoperabilitet og øget synergi mellem EU's informationssystemer (SIS, VIS og Eurodac).

SIS II består af en central database, der kaldes »det centrale Schengen-informationssystem« (CS-SIS), hvis operationelle forvaltning Kommissionen står for, og som er forbundet med nationale adgangspunkter for hver medlemsstat (NI-SIS). SIRENE-myndighederne sørger for udvekslingen af alle supplerende oplysninger (oplysninger forbundet med indberetninger i SIS II, som ikke lagres i SIS II).

Medlemsstaterne indsender data til SIS II om personer, der er eftersøgt med henblik på anholdelse, overgivelse eller udlevering, personer, der er eftersøgt med henblik på retsforfølgning, personer, der skal under overvågning eller underkastes særlig kontrol, personer, der skal nægtes indrejse ved de ydre grænser og forsvundne eller stjålne genstande. Et sæt oplysninger, der kaldes »indberetninger«, som indlæses i SIS II, gør det muligt for de kompetente myndigheder at identificere en person eller en genstand.

SIS II udvikler nye karakteristika: bredere adgang til SIS (Europol, Eurojust, offentlige anklagere, køretøjsregistreringsmyndigheder), sammenkobling af indberetninger, indsættelse af nye datakategorier, herunder biometriske data (fingeraftryk og fotografier) samt en teknisk platform, der er fælles med visuminformationssystemet. Disse nye elementer har i mange år givet anledning til diskussioner om en forskydning i formålet med SIS fra et kontrolinstrument hen imod et indberetnings- og efterforskningssystem.

1.2. **General vurdering af forslagene**

1. Den Europæiske Tilsynsførende for Databeskyttelse udtrykker sin tilfredshed med, at han er blevet hørt på grundlag af artikel 28, stk. 2, i forordning (EF) nr. 45/2001. I betragtning af den obligatoriske karakter af artikel 28, stk. 2, bør denne udtalelse imidlertid nævnes i præmblen til teksterne.

2. Den Europæiske Tilsynsførende for Databeskyttelse hilser forslagene velkommen af flere årsager. Den omstændighed at en mellemstatslig struktur omdannes til instrumenter i EU-retten har flere positive konsekvenser: den retlige værdi af SIS II-reglerne præciseres, Domstolen får kompetence vedrørende fortolkningen af retsakten under første søjle), Europa-Parlamentet bliver i det mindste delvis inddraget (omend lidt sent i processen).

3. Med hensyn til indholdet vedrører en betydelig del af forslagene regler om databeskyttelse, hvoraf nogle velkomne forbedringer sammenlignet med den nuværende situation. Man kan især nævne foranstaltningerne til fordel for ofre for identitetstyveri, udvidelsen af forordning 45/2001 til at omfatte Kommissionens databehandlingsaktiviteter under afsnit VI, en bedre definition af grundene til at indberette personer med henblik på nægtelse af indrejse.

4. Det er også klart, at man har været meget omhyggelig med udarbejdelsen af forslagene; de er komplekse, men dette afspejler kompleksiteten af det system, de omhandler. De fleste af bemærkningerne i denne udtalelse tager sigte på at præcisere eller supplere bestemmelserne, men de kræver ikke en fuldstændig omredigering.

Til trods for denne positive helhedsvurdering er der imidlertid visse forbehold især med hensyn til følgende:

1. Det er i mange henseender vanskeligt at vide, hvad der er hensigten bag teksten; det er højst beklageligt, at den ikke er ledsaget af en begrundelse. På grund af disse dokumenters meget komplekse karakter må en begrundelse betragtes som en basal nødvendighed. Mangelen derpå betyder, at læseren i nogle tilfælde ikke har andre muligheder end at gætte.

2. Desuden må man beklage, at der ikke er foretaget en konsekvensanalyse. Dette kan ikke begrundes med, at første udgave af systemet allerede er på plads, da der er betydelige forskelle mellem de to udgaver. Virkningen af indførelsen af biometriske oplysninger burde bl.a. være tænkt bedre igennem.

3. Rammen for den retlige databeskyttelse er meget kompleks; den er baseret på en kombineret anvendelse af *lex generalis* og *lex specialis*. Det bør sikres, at den eksisterende databeskyttelsesramme i direktiv 95/46/EF og forordning 45/2001 forbliver i kraft i fuld udstrækning, selv når der udvikles særlig lovgivning. Den kombinerede anvendelse af forskellige juridiske instrumenter bør hverken føre til forskelle mellem de nationale ordninger med hensyn til grundlæggende aspekter eller til sænkning af det nuværende databeskyttelsesniveau.

4. Det forhold, at mange nye myndigheder, der ikke har noget med det oprindelige »formål om kontrol med personer og genstande« at gøre, får adgang, bør ledsages af strengere garantier.

5. Forslagene er i betydeligt omfang baseret på andre retsakter, som fortsat er under udarbejdelse (somme tider endnu ikke foreslået). Den Europæiske Tilsynsførende for Databeskyttelse forstår, at det er vanskeligt at lovgive på et komplekst område, der er under konstant udvikling; under hensyn til konsekvenserne for de berørte personer og til den retlige usikkerhed, som det skaber, finder han imidlertid dette uacceptabelt.

6. Der er en del uklarhed i kompetencefordelingen mellem medlemsstaterne og Kommissionen. Klarhed er altafgørende og det er ikke kun nødvendigt for at systemet kan fungere smidigt, men også et grundlæggende krav for at sikre et omfattende tilsyn med systemet.

1.3. **Udtalelsens struktur**

Udtalelsen er struktureret således: Den præciserer først den retlige ramme for SIS II. Den omtaler derefter beskrivelsen af formålet med SIS II og de elementer, der adskiller sig væsentligt fra det nuværende system. Punkt 5 indeholder bemærkninger til Kommissionens og medlemsstaternes respektive roller i forbindelse med driften af SIS II. Punkt 6 vedrører de registreredes rettigheder, mens punkt 7 vedrører det nationale tilsyn og Den Europæiske Tilsynsførende for Databeskyttelses tilsyn samt samarbejdet mellem de tilsynsførende. Punkt 8 indeholder nogle bemærkninger og mulige ændringer vedrørende sikkerhed; punkt 9 og 10 handler om henholdsvis komitologi og interoperabilitet. Endelig fremhæver en oversigt over konklusionerne de vigtigste konklusioner for hvert punkt.

2. DEN RELEVANTE RETLIGE RAMME

2.1. **Den relevante databeskyttelsesramme for SIS II**

Forslagene henviser til direktiv 95/46/EF, konvention 108 og forordning 45/2001 som deres retlige databeskyttelsesramme. Andre instrumenter er også relevante.

For at gøre denne kontekst klarere og minde om de vigtigste referencepunkter for vor undersøgelse, er det hensigtsmæssigt at nævne følgende:

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

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

— Retten til respekt for privatliv og beskyttelse af personoplysninger er senere blevet fastlagt i artikel 7 og 8 i Den Europæiske Unions charter om grundlæggende rettigheder. Ifølge charterets artikel 52 anerkendes det, at disse rettigheder kan begrænses på samme betingelser som dem, der gælder i henhold til artikel 8 i EMRK.

— Det hedder i artikel 6, stk. 2, i EU-traktaten, at Unionen respekterer de grundlæggende rettigheder, således som de garanteres ved EMRK.

De tre tekster, der udtrykkeligt finder anvendelse på SIS II-forslagene, er følgende:

— Med Europarådets konvention nr. 108 af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (i det følgende benævnt »*konvention 108*«) er der udviklet grundlæggende principper for beskyttelse af det enkelte menneske i forbindelse med behandling af personoplysninger. Alle medlemsstaterne har ratificeret konvention 108. Den finder også anvendelse på aktiviteter, der udføres på det politimæssige og det retlige område. Konvention 108 er for øjeblikket den databeskyttelsesordning, der gælder for SIS-konventionen, sammen med anbefaling nr. R (87) 15 af 17. september 1987 fra Europarådets Ministerudvalg om politiets brug af personoplysninger.

— Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT L 281, s. 31). Dette direktiv benævnes i det følgende »*direktiv 95/46/EF*«. Det bør noteres, at den nationale lovgivning til gennemførelse af direktivet i de fleste af medlemsstaterne også omfatter databehandling på det politimæssige og det retlige område.

— Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger (EFT L 8, s.1). Denne forordning benævnes i det følgende »*forordning nr. 45/2001*«.

Fortolkningen af direktiv 95/46/EF og forordning 45/2001 må delvis afhænge af Den Europæiske Menneskerettighedsdomstols relevante retspraksis i henhold til EMRK. Med andre ord skal direktivet og forordningen, i det omfang de omhandler behandling af personoplysninger, der vil kunne krænke de grundlæggende frihedsrettigheder, navnlig retten til privatliv, fortolkes med udgangspunkt i de grundlæggende frihedsrettigheder. Dette følger også af EF-Domstolens retspraksis ([1]).

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

Kommissionen udsendte den 4. oktober 2005 et »forslag til Rådets rammeafgørelse om beskyttelse af personoplysninger i forbindelse med det politimæssige og strafferetlige samarbejde« ([1]) (i det følgende benævnt »*udkastet til rammeafgørelse*«). Denne rammeafgørelse skal erstatte konvention 108 som referencelovgivning for udkastet til afgørelse om SIS II, hvilket sandsynligvis vil have indvirkning på databeskyttelsesordningen i denne forbindelse (jf. 2.2.5).

2.2. **SIS II: den retlige ordning for databeskyttelse**

2.2.1. *Generelle bemærkninger*

Det nødvendige retlige grundlag for forvaltningen af SIS II består af særskilte instrumenter; som angivet i betragtningerne påvirker dette »ikke imidlertid princippet om, at SIS II udgør ét enkelt informationssystem, der skal fungere som sådant. Visse bestemmelser i disse instrumenter bør derfor være identiske«.

De to dokumenters struktur er i det store og hele den samme, idet kapitel I-III næsten er identiske. Det forhold, at SIS II skal ses som et enkelt informationssystem med to forskellige retsgrundlag afspejles også i den — temmelig komplekse — databeskyttelsesordning.

Databeskyttelsesordningen fastlægges delvis i selve forslagene som en »*lex specialis*« suppleret med en særskilt referencelovgivning (»*lex generalis*«) for hver enkelt sektor (Kommissionen, medlemsstaterne i første søjle, medlemsstaterne i tredje søjle).

Denne struktur rejser spørgsmålet om, hvordan særlige regelsæt forholder sig til den generelle ret. Den Europæiske Tilsynsførende for Databeskyttelse anser i dette tilfælde den særlige regel for at være en anvendelse af den generelle regel.

Som følge heraf skal *lex specialis* altid være i overensstemmelse med *lex generalis*; den uddyber (specificerer eller udvider) *lex generalis*, men opfattes ikke som en undtagelse herfra. Med hensyn til spørgsmålet om, hvilken regel der skal anvendes i bestemte tilfælde, er princippet, at *lex specialis* gælder først; men når den ikke siger noget eller er uklar, skal der henvises til *lex generalis*.

Med denne struktur er der tre forskellige kombinationer af *lex generalis* og *lex specialis*. De kan sammenfattes således:

2.2.2. *Den ordning, der gælder for Kommissionen*

Når Kommissionen er involveret, finder forordning 45/2001 anvendelse, herunder også Den Europæiske Tilsynsførende for Databeskyttelses rolle, uanset om aktiviteterne udføres inden for rammerne af første (den foreslåede forordning) eller tredje søjle (den foreslåede afgørelse). Betragtning 21 i den foreslåede afgørelse fastsætter, at »forordning (EF) nr. 45/2001 (…) finder anvendelse på Kommissionens behandling af personoplysninger, når denne behandling sker i forbindelse med gennemførelsen af aktiviteter, der helt eller delvis falder ind under fællesskabsretten. En del af behandlingen af personoplysninger i SIS II falder ind under fællesskabsretten.«

Der er praktiske årsager hertil: det ville faktisk være meget vanskeligt, for så vidt angår Kommissionen, at afgøre, om dataene behandles inden for rammerne af aktiviteter, der falder ind under lovgivning i første eller tredje søjle.

Desuden giver det ikke blot mere mening set ud fra et praktisk synspunkt at anvende ét juridisk instrument på alle Kommissionens aktiviteter i forbindelse med SIS II, det forbedrer også sammenhængen (idet det i overensstemmelse med betragtning 21 i den foreslåede forordning sikrer »en sammenhængende og ensartet anvendelse af reglerne for beskyttelse af fysiske personers grundlæggende rettigheder og friheder for så vidt angår behandling af personoplysninger«). Derfor er Den Europæiske Tilsynsførende for Databeskyttelse tilfreds med Kommissionens erkendelse af, at forordning 45/2001 finder anvendelse på alle Kommissionens databehandlingsaktiviteter under SIS II.

2.2.3. *Den ordning, der gælder for medlemsstaterne*

Situationen er mere kompleks for medlemsstaternes vedkommende. Behandlingen af personoplysninger i henhold til den foreslåede forordning reguleres af selve den foreslåede forordning samt direktiv 95/46/EF. Betragtning 14 i den foreslåede forordning gør det meget klart, at direktivet skal betragtes som *lex generalis*, mens SIS II-forordningen er *lex specialis*. Dette har nogle konsekvenser, som præciseres i det følgende.

Med hensyn til den foreslåede afgørelse er det juridiske instrument for databeskyttelse, der henvises til (*lex generalis*), konvention 108, hvilket kan medføre stor forskel mellem databeskyttelsesordningerne under første og tredje søjle på visse punkter.

2.2.4. *Virkningen på databeskyttelsesniveauet*

Som generel bemærkning til denne databeskyttelsesarkitektur understreger Den Europæiske Tilsynsførende for Databeskyttelse følgende:

— Anvendelsen af den foreslåede forordning som *lex specialis* for direktiv 95/46/EF (og tilsvarende af den foreslåede afgørelse som *lex specialis* for konvention 108) må aldrig medføre en sænkning af det databeskyttelsesniveau, der sikres med direktivet eller konventionen. Den Europæiske Tilsynsførende for Databeskyttelse vil fremsætte henstillinger herom (se f.eks. klageadgang).

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

— På samme måde kan den kombinerede anvendelse af juridiske instrumenter ikke medføre, at det databeskyttelsesniveau, der sikres i den nuværende Schengen-konvention, sænkes (se f.eks. bemærkningerne i det følgende til artikel 13 i direktiv 95/46/EF).

— Anvendelsen af to forskellige instrumenter må, selv om det er nødvendigt på grund af EU-retten, ikke medføre uberettigede forskelle mellem databeskyttelsen af de berørte personer alt efter den type data, der behandles om dem. Dette skal undgås i så vidt omfang som muligt. Det vil i henstillingerne i det følgende også blive forsøgt at forbedre sammenhængen så meget som muligt (se f.eks. de nationale tilsynsmyndigheders beføjelser).

— Den retlige ramme er så kompleks, at det meget vel kan føre til en vis forvirring ved den praktiske anvendelse. Det er i nogle tilfælde vanskeligt at se, hvordan *lex generalis* og *lex specialis* forholder sig til hinanden, og det ville være nyttigt at afklare dette i forslagene. I denne komplekse retlige sammenhæng er det forslag, som Den Fælles Tilsynsmyndighed for Schengen fremsætter i sin udtalelse vedrørende det foreslåede retsgrundlag for SIS II (27. september 2005) om at udvikle et »vademecum« med en liste over alle de rettigheder, der eksisterer i forbindelse med SIS II og med et klart hierarki for den gældende lovgivning, meget nyttigt.

Som konklusion vil denne udtalelse stræbe mod at sikre et højt niveau af databeskyttelse, sammenhæng og klarhed for at give den registrerede den nødvendige retssikkerhed.

2.2.5. *Virkningen af udkastet til rammeafgørelse på databeskyttelsen i tredje søjle*

Konvention 108 vil som referenceinstrument for databeskyttelse for udkastet til afgørelse om SIS II blive erstattet med rammeafgørelsen om databeskyttelse i tredje søjle [1]. Dette nævnes ikke i forslaget, men følger af den foreslåede rammeafgørelse. Artikel 34, stk. 2, har følgende ordlyd: »Alle henvisninger til Europarådets konvention nr. 108 af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger læses som en henvisning til denne rammeafgørelse.« Den Europæiske Tilsynsførende for Databeskyttelse vil i løbet af de kommende uger udsende en udtalelse om udkastet til rammeafgørelse og vil ikke analysere indholdet i detaljer i denne udtalelse. Hvor anvendelsen af rammeafgørelsen vil kunne have en betydelig virkning på databeskyttelsesordningen for SIS II, vil dette dog blive nævnt.

2.2.6. *Anvendelsen af artikel 13 i direktiv 95/46/EF og artikel 9 i konvention 108*

Artikel 13 i direktiv 95/46/EF og artikel 9 i konvention 108 giver medlemsstaterne mulighed for at træffe lovmæssige foranstaltninger med henblik på at begrænse rækkevidden af de forpligtelser og rettigheder, de har indført, hvis en sådan begrænsning er en nødvendig foranstaltning af hensyn til andre vigtige interesser (f.eks. statens sikkerhed, forsvaret, den offentlige sikkerhed) [2].

Betragtningerne i både den foreslåede forordning og den foreslåede afgørelse nævner, at medlemsstaterne kan anvende denne mulighed, når de gennemfører forslagene på nationalt plan. To krav skal i så tilfælde være opfyldt: anvendelsen af artikel 13 i direktiv 95/46/EF skal være i overensstemmelse med artikel 8 i EMRK og må ikke medføre en svækkelse af de nuværende databeskyttelsesordning.

Dette er endnu vigtigere i forbindelse med SIS II, da systemet skal have en forudsigelig karakter. Da medlemsstaterne udveksler oplysninger, skal der være mulighed for rimeligt sikkert at vide, hvordan de vil blive behandlet på nationalt plan.

Der er især ét problematisk element i denne forbindelse, hvor forslagene ville føre til en sænkning af det nuværende databeskyttelsesniveau. Artikel 102 i Schengen-konvention omhandler et system, hvor anvendelsen af oplysninger er strengt reguleret og begrænset, selv i den nationale lovgivning (»Enhver anvendelse af oplysninger i strid med stk. 1-4 skal betragtes som misbrug efter bestemmelserne i den pågældende kontraherende parts nationale lovgivning«). Både direktiv 95/46/EF og konvention 108 fastsætter imidlertid, at der kan indføres undtagelser fra bl.a. princippet om formålsbegrænsning i den nationale lovgivning. Hvis dette sker, vil systemet ikke være i overensstemmelse med det nuværende system i Schengen-konventionen, hvor den nationale lovgivning ikke kan fravige kerneprincippet om begrænsning af formål og anvendelse.

Vedtagelsen af rammeafgørelsen vil ikke ændre dette: problemet er snarere at bevare et strengt formålsbegrænsningsprincip ved behandling af SIS II-oplysninger end at sikre, at oplysninger behandles i overensstemmelse med rammeafgørelsen.

[1] Den vil også erstatte den generelle databeskyttelsesordning i Schengen-konventionen (artikel 126-130 i Schengen-konventionen). Denne ordning gælder ikke for SIS.

[2] En medlemsstat, der anvender denne mulighed for at begrænse rettigheder, kan som allerede nævnt kun gøre dette i overensstemmelse med artikel 8 i EMRK.

Den Europæiske Tilsynsførende for Databeskyttelse foreslår, at der i SIS II-forslagene (dvs. artikel 21 i den foreslåede forordning og artikel 40 i den foreslåede afgørelse) indsættes en bestemmelse med samme virkning som den nuværende artikel 102, stk. 4, i Schengen-konventionen, idet den begrænser medlemsstaternes mulighed for at indføre anvendelser af data, som ikke forekommer i SIS II-teksterne. En anden mulighed for udtrykkeligt i den foreslåede afgørelse og den foreslåede forordning at begrænse rækkevidden af de undtagelser, der kan anvendes i henhold til artikel 13 i direktivet eller artikel 9 i konventionen, vil være f.eks. at fastsætte, at medlemsstaterne kun kan begrænse retten til adgang og information, men ikke principperne om datakvalitet.

3. **FORMÅL**

Ifølge artikel 1 i de to dokumenter (»Oprettelse af SIS II og generelle mål«) oprettes SIS II »for at sætte medlemsstaternes kompetente myndigheder i stand til at samarbejde ved at udveksle oplysninger med henblik på at kontrollere personer og genstande«, og det »bidrager til at opretholde et højt sikkerhedsniveau i et område uden kontrol ved de indre grænser mellem medlemsstaterne.«

Formålet med SIS II er formuleret temmelig generelt; ovennævnte bestemmelser er ikke i sig selv en præcis angivelse af, hvad der er omfattet af (menes med) dette mål.

Formålet med SIS II synes at være meget bredere end formålet med det nuværende SIS som fastsat i artikel 92 i Schengenkonventionen, som især henviser til »(…) adgang til indberetninger om personer og genstande til brug for grænsekontrollen og for anden politi- og toldkontrol (…) samt, kun hvad angår den type indberetning, der er nævnt i artikel 96, til brug for proceduren for visumudstedelse, udstedelse af opholdstilladelser og håndhævelse af udlændingelovgivningen (…)«.

Dette bredere formål skyldes også, at der i SIS II er indført nye funktioner og adgange, som ikke svarer til det oprindelige formål, som var kontrol med personer og genstande, men mere til formålet med et efterforskningsredskab. Der fastsættes især adgang for myndigheder, som vil anvende SIS II-oplysninger til deres egne formål og ikke til opfyldelse af SIS II-formålene (se nedenfor); sammenkobling af indberetninger vil blive almindeligt, mens dette typisk er et led i anvendelsen af et politiefterforskningsredskab.

Der er også udestående spørgsmål vedrørende den biometriske søgemaskine, der skal udvikles i de kommende år og give mulighed for søgninger i systemet, som går videre end behovene i et kontrolsystem.

Som konklusion har forslagene et meget bredere anvendelsesområde end den nuværende ramme. Dette kræver yderligere garantier. I denne forbindelse vil Den Europæiske Tilsynsførende for Databeskyttelse fokusere sin analyse ikke så meget på den brede definition i artikel 1 som sådan, men på SIS II's funktioner og andre bestanddele.

4. **BETYDELIGE ÆNDRINGER I SIS II**

Dette kapitel fokuserer først på de nye elementer, som indføres med SIS II, nemlig biometri, den nye opfattelse af adgang, med særlig opmærksomhed på adgang for Europol og Eurojust, for de myndigheder, der har ansvaret for køretøjsregistrering, sammenkobling af indberetninger og forskellige myndigheders adgang til oplysninger om indvandring.

4.1. **Biometri**

SIS II-forslagene indfører mulighed for at behandle en ny kategori af oplysninger, som fortjener særlig opmærksomhed: biometriske oplysninger. Som allerede understreget i udtalelsen fra Den Europæiske Tilsynsførende for Databeskyttelse om visuminformationssystemet [1] kræver biometriske oplysningers følsomme art særlige garantier, som ikke er indeholdt i SIS II-forslagene.

Generelt set er tendensen til at anvende biometriske oplysninger i de EU-omfattende informationssystemer (VIS, Eurodac, informationssystemet om kørekort, osv.) jævnt tiltagende, men er ikke ledsaget af en omhyggelig overvejelse af risikoen og de nødvendige garantier.

Dette behov for en nøjere overvejelse blev også fremhævet i den nylige resolution om biometri, der blev udsendt af den internationale konference mellem datatilsynsmyndighederne i Montreux [2]. Hidtil har man kun fokuseret på den stigende interoperabilitet mellem systemerne og ikke på forbedringen af kvaliteten af de biometriske processer, når man har talt om merværdien i forbindelse med udvikling af standarder.

---

[1] Udtalelsen fra Den Europæiske Tilsynsførende for Databeskyttelse om forslaget til Europa-Parlamentets og Rådets forordning om visuminformationssystemet (VIS) og udveksling af oplysninger mellem medlemsstaterne om visa til kortvarigt ophold af 23. marts 2005, punkt 3.4.2.

[2] 27. internationale konference mellem datatilsynsmyndighederne den 16. september 2005 i Montreux, resolution om anvendelsen af biometri i pas, identitetskort og rejsedokumenter.

Det ville være nyttigt at opbygge et sæt af fælles forpligtelser eller krav i forbindelse med disse oplysningers specificitet samt en fælles metode til gennemførelse deraf. Disse fælles krav kunne især indeholde følgende elementer (behovet herfor fremgår af SIS II-forslagene):

— **Målrettet konsekvensanalyse:** Det skal understreges, at der ikke er foretaget en konsekvensanalyse af forslagene med hensyn til anvendelsen af biometri ([1]).

— **Vægt på registreringsproceduren:** Kilden til biometriske oplysninger og den måde, hvorpå de indsamles, er ikke angivet. Registreringen er et kritisk skridt i den samlede procedure for biometrisk identifikation og kan ikke blot fastlægges i bilag eller ved yderligere drøftelser i undergrupper, da den vil være direkte bestemmende for det endelige resultat af proceduren, dvs. fejlafvisningsfrekvensen eller fejlgodkendelsesfrekvensen.

— **Fremhævelse af nøjagtigheden**: Anvendelsen af biometri til identifikation (»en-til-mange«-sammenligning), der forelægges i forslaget som en fremtidig gennemførelse af en »biometrisk søgemaskine« er mere kritisk, da resultaterne af denne procedure er mindre nøjagtige end anvendelsen til autentificering eller kontrol (»en-til-en«-sammenligning). Biometrisk identifikation bør derfor ikke være den eneste identifikationsmåde eller eneste adgangsnøgle til yderligere oplysninger.

— **Tilbagefaldsprocedure.** Der bør gennemføres let tilgængelige tilbagefaldsprocedurer for at respektere værdigheden af personer, som kunne være blevet fejlidentificeret, og for at undgå, at de belastes af manglerne ved systemet.

Anvendelsen af biometriske oplysninger uden en egentlig foregående vurdering viser også, at biometriens pålidelighed overvurderes. Biometriske oplysninger er »levende« data, der udvikler sig med tiden; de data, som lagres i databasen, udgør kun et øjebliksbillede af et dynamisk element. Det er ikke absolut uforanderligt og skal kontrolleres. Biometriens nøjagtighed skal altid sættes i perspektiv ved hjælp af andre elementer, da den aldrig vil være absolut.

([1]) Analysen kan baseres på de såkaldte syv piller af biometrisk visdom i »Biometrics at the frontiers: assessing the impact on Society«, IPTS, GD-FFC, EUR 21585 EN, del 1.2, side 32.

Den eventuelle anvendelse af SIS II-data til efterforskningsformål medfører alvorlige risici for den registrerede, hvis man tillægger biometrisk materiale en større eller en overvurderet betydning, som det er blevet påvist i tidligere tilfælde ([2]).

Det bør derfor fremgå af forslagene, at man erkender de reelle muligheder, som biometrien giver i forbindelse med identifikation, men man bør også henlede opmærksomheden på farerne derved.

4.2. **Adgangen til oplysninger i SIS II**

4.2.1 *Et nyt syn på adgang*

De myndigheder, der har adgang til SIS-oplysninger, fastlægges for hver indberetning. Der stilles i princippet to krav for at få adgang til SIS-data: adgangen skal gives til myndighederne i fuld overensstemmelse med det generelle formål med SIS og med det særlige formål med hver indberetning.

Dette følger af definitionen af indberetning i både den foreslåede forordning og den foreslåede afgørelse (artikel 3, stk. 1, litra a) i begge instrumenter: *»indberetning«: et sæt oplysninger, der indlæses i SIS II, således at de kompetente myndigheder kan identificere en person eller en genstand med henblik på at træffe en særlig foranstaltning)*. Artikel 39, stk. 3, i den foreslåede afgørelse styrker dette synspunkt, idet det hedder, at *»de oplysninger, der er omhandlet i stk. 1, anvendes i overensstemmelse med denne afgørelse kun til at identificere en person med henblik på en særlig foranstaltning, der skal træffes«*. I denne henseende har SIS II fortsat de karakteristika, der forbindes med et hit/no hit-system, hvor hver enkelt indberetning indsættes med et bestemt formål (overgivelse, nægtelse af indrejse, …).

De myndigheder, der har adgang til SIS-data, er undergivet en de facto begrænsning i anvendelsen af disse data, da de i princippet kun kan få adgang til dem med henblik på en særlig foranstaltning.

Nogle adgange i de nye forslag følger imidlertid ikke denne logik: de tager sigte på at give myndigheden oplysninger, men ikke på at gøre det muligt for den at identificere en person og træffe den foranstaltning, der påtænkes med indberetningen.

([2]) I juni 2004 blev en advokat fra Portland (USA) fængslet i to uger, fordi FBI med held matchede hans fingeraftryk med et, der blev fundet efter terrorbombeangrebet i Madrid (på den plasticpose, som indeholdt detonatoren). Det blev til sidst påvist, at der var begået fejl under matchingen, som førte til en misfortolkning.

Dette vedrører mere specifikt:

— asylmyndigheders adgang til indvandringsdata

— adgang til indvandringsdata for de myndigheder, der har ansvaret for at indrømme flygtningestatus

— adgang til indberetninger om udlevering, diskret overvågning og stjålne dokumenter til beslaglæggelse for Europol

— adgang til data om udlevering og lokalisering for Eurojust.

Alle disse myndigheder har samme karakteristika med hensyn til SIS II-data: de kan ikke træffe den særlige foranstaltning, der er nævnt i definitionen af indberetning. De får adgang til en kilde til oplysninger, som de anvender til deres egne formål.

For så vidt angår disse myndigheder, skal der sondres mellem dem, der har adgang til at anvende oplysningerne til deres egne formål, men med et temmelig specifikt mål, og dem (Europol og Eurojust), for hvilke der slet ikke er specificeret noget formål med adgangen.

Asylmyndigheder har for eksempel adgang med et særligt formål, selv om det ikke er det formål, der nævnes i indberetningen. De kan have adgang til indvandringsdata »for at afgøre, om en asylansøger ulovligt har opholdt sig i en anden medlemsstat.« Europol og Eurojust har imidlertid adgang til data, som findes i visse kategorier af indberetninger, »der er nødvendige for, at de kan udføre deres opgaver«.

Sammenfattende kan det siges, at der er adgang til SIS II-oplysninger i tre tilfælde:

— adgang for at opfylde formålet med indberetningen

— adgang med et andet formål end SIS II, som klart er omfattet af forslagene

— adgang med et andet formål end SIS II, som ikke er præcist beskrevet.

Den Europæiske Tilsynsførende for Databeskyttelse mener, at jo mere generelt formålet med adgangen er, jo større garantier skal der fastsættes. De generelle garantier er angivet i det følgende; derefter vil Europols og Eurojusts særlige situation blive behandlet.

4.2.2. *Adgangsbetingelser*

1. Der kan under alle omstændigheder kun gives adgang, når det er foreneligt med det generelle formål med SIS II og i overensstemmelse med dets retsgrundlag.

   Dette betyder i praksis, at adgang til indvandringsoplysninger i henhold til den foreslåede forordning skal støtte gennemførelsen af politikker, der er forbundet med personers bevægelighed som led i Schengen-reglerne.

   På samme måde skal adgang til indberetninger i henhold til afgørelsen tage sigte på at støtte det operationelle samarbejde mellem politimyndigheder og retsmyndigheder i forbindelse med straffesager.

   I denne henseende henleder Den Europæiske Tilsynsførende for Databeskyttelse opmærksomheden på kapitlet om adgang til SIS II for de myndigheder, der har ansvaret for at udstede registreringsattester (jf. punkt 4.6).

2. Det skal påvises, at der er behov for adgang til SIS II-data, samt at det er umuligt eller meget vanskeligt at få oplysningerne på andre mindre indgribende måder. Dette burde være gjort i en begrundelse, og det er som allerede nævnt meget beklageligt, at der ikke findes en sådan.

3. Brugen af oplysningerne skal beskrives udtrykkeligt og restriktivt.

   For eksempel har asylmyndigheder adgang til indvandringsoplysninger »for at afgøre, om en asylansøger ulovligt har opholdt sig i en anden medlemsstat.« Europol og Eurojust har imidlertid adgang til de data, som findes i visse kategorier af indberetninger, »der er nødvendige for, at de kan udføre deres opgaver«; dette er ikke tilstrækkelig præcist (se nedenfor).

4. Betingelserne for adgang skal være fastlagt præcist og være begrænsede. Især må kun de tjenester inden for disse organisationer, som skal arbejde med SIS II-dataene, have adgang hertil. Denne bestemmelse, som er fastsat i artikel 40 i den foreslåede afgørelse og artikel 21, stk. 2, i den foreslåede forordning, skal suppleres med en bestemmelse om, at de nationale myndigheder har pligt til at føre en ajourført liste over de personer, der har ret til at få adgang til SIS II. Det samme skal gælde for Europol og Eurojust.

5. Det forhold, at disse myndigheder får adgang til SIS II-oplysninger, kan aldrig være en grund til at indlæse eller bevare oplysninger i systemet, hvis de ikke er nyttige for den bestemte indberetning, som de er en del af. Der må ikke tilføjes nye kategorier af oplysninger, fordi de ville være til fordel for andre informationssystemer. For eksempel hedder det i artikel 39 i den foreslåede afgørelse, at der skal indsættes oplysninger i indberetninger om den myndighed, der foretager indberetningen. Sådanne oplysninger er ikke nødvendige for at træffe en foranstaltning (arrestation, overvågning, …) og den eneste årsag til, at de kan indsættes, er sandsynligvis at de vil være til gavn for Europol eller Eurojust. Der skal gives en klar begrundelse for behandling af sådanne oplysninger.

6. Det tidsrum, hvor oplysningerne bevares, kan ikke forlænges, hvis det ikke er nødvendigt for det formål, til hvilket oplysningerne er indsat. Dette betyder, at selv om Europol eller Eurojust har adgang til disse oplysninger, er dette ikke en tilstrækkelig grund til at bevare dem i systemet (for eksempel skal oplysningerne slettes, når en eftersøgt person er blevet udleveret, selv om de kunne være nyttige for Europol). Også her vil det vær nødvendigt med omhyggelig overvågning for at sikre, at de nationale myndigheder overholder dette.

4.2.3. *Adgang for Europol og Eurojust*

a. *Grunde til adgang*

Europols og Eurojusts adgang til nogle SIS-oplysninger var allerede blevet drøftet, før de blev omfattet af Rådets afgørelse af 24. februar 2005 ([1]). Blandt alle de myndigheder, der har adgang med deres egne formål, har de adgang på de mest åbne betingelser. Selv om anvendelsen af disse data er beskrevet i kapitel VII i afgørelsen, er grundene til overhovedet at give adgang ikke tilstrækkelig udbyggede. Dette er endnu tydeligere, når man tager i betragtning, at Europols og Eurojusts opgaver sandsynligvis vil udvikle sig med tiden.

Den Europæiske Tilsynsførende for Databeskyttelse anmoder indtrængende Kommissionen om restriktivt at fastlægge de opgaver, hvis udførelse berettiger adgang for Europol og Eurojust.

b. *Databegrænsning*

For at undgå, at Europol og Eurojust foretager »fishing expeditions« og for at sikre, at de kun får adgang til oplysninger, »der er nødvendige for, at de kan udføre deres opgaver«, foreslog Den Fælles Tilsynsmyndighed for Schengen i sin udtalelse af 27. september 2005 om SIS II-forslagene, at Europols og Eurojusts adgang begrænses til oplysninger om personer, hvis navne allerede findes i deres filer. Dette ville sikre, at de kun konsulterer indberetninger, der er relevante for dem. Den Europæiske Tilsynsførende for Databeskyttelse støtter denne henstilling.

c. *Sikkerhedsaspekter*

Den Europæiske Tilsynsførende for Databeskyttelse ser med tilfredshed på, at der er pligt til at køre logfiler for alle transaktioner i forbindelse med Europol og Eurojust, samt at det er forbudt at kopiere eller downloade dele af systemet.

Artikel 56 i den foreslåede afgørelse fastsætter »et eller to« adgangspunkter for Europol og Eurojust. Selv om man kan forstå, at en medlemsstat kan have brug for mere end et adgangspunkt på grund af en decentraliseret opbygning af dens kompetente myndigheder, berettiger Europols og Eurojusts status og aktiviteter ikke dette ønske. Det skal også understreges, at set ud fra et sikkerhedssynspunkt øger flere adgangspunkter risikoen for misbrug, og det bør derfor begrundes nøje med mere relevante elementer. Da der ikke foreligger en overbevisende argumentation, foreslår Den Europæiske Tilsynsførende for Databeskyttelse, at Europol og Eurojust kun får ét adgangspunkt.

4.3. **Sammenkobling af indberetninger**

Det hedder i artikel 26 i forordningen og artikel 46 i afgørelsen, at medlemsstaterne kan sammenkoble indberetninger i overensstemmelse med national lovgivning for at skabe en forbindelse mellem to eller flere indberetninger.

Selv om sammenkobling af indberetninger kan være nyttigt i forbindelse med kontrol (f.eks. kan en arrestordre for en biltyv sammenkobles med et stjålet køretøj), er indførelsen af sammenkobling af indberetninger en meget typisk karakteristika for et politiefterforskningsredskab.

Sammenkobling af indberetninger kan have en stor virkning på den berørte persons rettigheder, da vedkommende ikke længere »vurderes« udelukkende på grundlag af oplysninger om ham/hende selv, men på grundlag af hans/hendes eventuelle forbindelse med andre personer. Personer, hvis data sammenkobles med kriminelle eller eftersøgte personers data, vil sandsynligvis blive behandlet med mere mistænksomhed end andre. Sammenkobling af indberetninger udgør desuden en udvidelse af SIS's efterforskningsbeføjelser, fordi det vil gøre det muligt at registrere påståede bander eller netværker (hvis for eksempel oplysninger om ulovlige indvandrere sammenkobles med oplysninger om menneskesmuglere). Da skabelsen af forbindelser overlades til den nationale lovgivning, er det en mulig konsekvens, at sammenkoblinger, som er ulovlige i én medlemsstat, kan foretages af en anden, og at der således indsættes »ulovlige« data i systemet.

([1]) Rådets afgørelse 2005/211/RIA af 24. februar 2005 om indførelse af nye funktioner i Schengen-informationssystemet, bl.a. med henblik på terrorismebekæmpelse, EUT L 68/44 af 15.3.2005.

Ifølge Rådets konklusioner af 14. juni 2004 om funktionskravene til SIS II skal hvert link opfylde klare operationelle behov, være baseret på et klart defineret forhold og respektere proportionalitetsprincippet. Desuden må det ikke berøre adgangsretten. Da sammenkobling af indberetninger udgør en behandlingsoperation, skal den under alle omstændigheder være i overensstemmelse med bestemmelserne i den nationale lovgivning om gennemførelse af direktiv 95/46/EF og/eller konvention 108.

Det gentages i forslagene, at eksistensen af links ikke kan ændre adgangsrettighederne (ellers ville dette give adgang til data, som det ikke ville være lovligt at behandle i henhold til den nationale lovgivning, i modstrid med artikel 6 i direktivet).

Den Europæiske Tilsynsførende for Databeskyttelse understreger betydningen af en streng fortolkning af artikel 26 i den foreslåede forordning og artikel 46 i den foreslåede afgørelse: dette kan f.eks. sikres ved, at det gøres klart, at myndigheder, der ikke har adgang til visse kategorier af oplysninger, ikke blot er udelukket fra at få adgang til links til disse kategorier, men at de heller ikke må have kendskab til eksistensen af disse links. Det skal være umuligt at se disse links, hvis der ikke er nogen adgangsret til de sammenkoblede data.

Desuden vil Den Europæiske Tilsynsførende for Databeskyttelse gerne høres om de tekniske foranstaltninger til at sikre dette.

4.4. **Indberetninger med henblik på indrejseforbud**

4.4.1. *Grunde til medtagelse*

Anvendelsen af »indberetninger vedrørende tredjelandsstatsborgere med henblik på indrejseforbud« (artikel 15 i forordningen) har en betydelig indvirkning på personens frihedsrettigheder: en person, der er indberettet i henhold til denne bestemmelse, har ikke adgang til Schengen-området i flere år. Dette har hidtil været den mest brugte indberetning, når man ser på antallet af indberettede personer. På grund af konsekvenserne af denne indberetning samt antallet af berørte personer må man være meget omhyggelig med dens udformning samt gennemførelse. Selv om dette også gælder for andre indberetninger, vil Den Europæiske Tilsynsførende for Databeskyttelse behandle denne form for indberetning i et særligt kapitel, fordi den giver specifikke problemer i forbindelse med grundene til medtagelse.

Den nye indberetning med henblik på indrejseforbud udgør en forbedring i forhold til den nuværende situation, men den er heller ikke helt tilfredsstillende, da den for en stor del er baseret på instrumenter, som endnu ikke er vedtaget eller sågar foreslået.

Forbedringerne ligger i en mere præcis beskrivelse af grundene til at medtage oplysninger. Den nuværende affattelse af Schengen-konventionen har ført til en situation, hvor der er betydelige forskelle mellem medlemsstaterne med hensyn til det antal personer, der indberettes i henhold til artikel 96 i konventionen. Den Fælles Tilsynsmyndighed for Schengen har foretaget en omfattende undersøgelse ([1]) af spørgsmålet og fremsat henstillinger om, at beslutningstagerne overvejer at harmonisere årsagerne til at foretage en indberetning i de forskellige Schengen-stater.

Den foreslåede artikel 15 er mere detaljeret i sin udformning, hvilket må betragtes som tilfredsstillende.

Desuden indeholder artikel 15, stk. 2, også en liste over tilfælde, hvor personer ikke kan indberettes, fordi de opholder sig lovligt på en medlemsstats område med forskellige former for status. Selv om det kan udledes af den nuværende Schengen-konvention, har praksis vist, at anvendelsen af denne mekanisme også varierer mellem medlemsstaterne. Derfor er præciseringen et positivt element.

Der rettes imidlertid også alvorlig kritik mod denne bestemmelse, fordi den for en stor del er baseret på en endnu ikke vedtaget tekst, nemlig direktivet om tilbagesendelse.

Siden vedtagelsen af SIS II-forslagene har Kommissionen foreslået et »direktiv om fælles standarder og procedurer i medlemsstaterne for tilbagesendelse af tredjelandsstatsborgere med ulovligt ophold« (1. september 2005), men så længe teksten ikke er endelig, kan den ikke betragtes som gyldig grund til at indsætte data i systemet. Dette ville være et brud på især artikel 8 i EMRK, da indgriben i personers privatliv skal være berettiget ved — bl.a. — klar og tilgængelig lovgivning.

Den Europæiske Tilsynsførende for Databeskyttelse anmoder derfor indtrængende Kommissionen om enten at trække denne bestemmelse tilbage eller at omarbejde den på grundlag af eksisterende lovgivning, således at en person kan vide, nøjagtig hvilke foranstaltninger myndighederne kan træffe mod ham/hende.

4.4.2. *Adgang til artikel 15-indberetninger*

Artikel 18 fastsætter, hvilke myndigheder, der har adgang til disse indberetninger og til hvilke formål. Artikel 18, stk. 1 og 2, fastsætter, hvilke myndigheder, der har adgang til indberetninger, der er indlæst på grundlag af direktivet om tilbagesendelse. Der gælder samme kommentar som ovenfor.

([1]) Rapport fra Den Fælles Tilsynsmyndighed for Schengen om en undersøgelse af anvendelsen af artikel 96-indberetninger i Schengen-informationssystemet, Bruxelles, den 20. juni 2005.

Artikel 18, stk. 3, i den foreslåede forordning giver adgang for de myndigheder, der har ansvaret for at indrømme flygtningestatus, i henhold til et direktiv, som end ikke er blevet foreslået endnu. Da der ikke foreligger en tilgængelig tekst, må Den Europæiske Tilsynsførende for Databeskyttelse gentage de ovenfor anførte bemærkninger.

4.4.3. *Tidsrum for bevaring af artikel 15-indberetninger*

En indberetning må ifølge artikel 20 ikke bevares længere end det tidsrum, hvori beslutningen om indrejseforbud gælder (udsendelse eller tilbagesendelse). Dette er i overensstemmelse med databeskyttelsesreglerne. Endvidere slettes indberetningen automatisk efter fem år, med mindre den medlemsstat, der har indsat oplysningen i SIS II, træffer anden afgørelse.

Et passende tilsyn på nationalt plan skal sikre, at der ikke automatisk sker en uberettiget forlængelse af tidsrummet for bevaring, og at medlemsstaterne sletter oplysningen, inden der er gået fem år, hvis indrejseforbuddet var for et kortere tidsrum.

4.5. **Tidsrum for bevaring**

Selv om princippet om bevaring forbliver det samme (generelt skal en indberetning slettes i SIS II, så snart den foranstaltning, der kræves i indberetningen, er truffet), vil forslagene resultere i, at tidsrummet for bevaring af indberetningerne generelt forlænges.

Schengen-konventionen indeholder bestemmelser om en ny undersøgelse af behovet for fortsat lagring af oplysningerne senest tre år efter, at de er indsat (eller et år i tilfælde af data, der er indsat med henblik på diskret overvågning). Ifølge de nye forslag skal der foretages automatisk sletning (med mulighed for indsigelse fra den medlemsstat, der har foretaget indberetningen) efter 5 år for indvandringsoplysninger, 10 år for oplysninger om arrest, forsvundne personer og personer, der er eftersøgt med henblik på retlige procedurer, og 3 år for personer, der skal sættes under diskret overvågning.

Selv om medlemsstaterne i princippet vil skulle slette oplysningerne, når formålet med indberetningen er opfyldt, indebærer dette en betydelig forlængelse af det maksimale tidsrum for bevaring (i de fleste tilfælde en tredobling), uden at Kommissionen begrunder det på nogen måde. I forbindelse med indvandringsoplysninger kan man kun gætte på, at tidsrummet på 5 år er forbundet med indrejseforbuddets varighed som foreslået i udkastet til direktiv om tilbagesendelse. I alle andre tilfælde er der, så vidt Den Europæiske Tilsynsførende for Databeskyttelse ved, ikke nogen begrundelse.

Den potentielle virkning for de registrerede, der bliver indberettet i SIS, kan få betydelige konsekvenser for de berørte personers liv. Dette er særlig foruroligende i tilfælde af indberetninger om personer med henblik på diskret overvågning eller særlig kontrol, da disse indberetninger kan være foretaget på grundlag af mistanker.

Den Europæiske Tilsynsførende for Databeskyttelse vil gerne have en seriøs begrundelse for denne forlængelse af tidsrummene for bevaring af oplysninger. Hvis der ikke er nogen overbevisende begrundelse, foreslår han, at de begrænses til deres nuværende varighed, og fremhæver især indberetninger med henblik på diskret overvågning eller særlig kontrol.

4.6. **Adgang for de myndigheder, der har ansvaret for udstedelse af registreringsattester for køretøjer**

Det vigtigste spørgsmål er valget af et mere end anfægteligt retsgrundlag. Kommissionen argumenterer ikke overbevisende nok for anvendelsen af et retsgrundlag vedrørende »transport« under første søjle for en foranstaltning, som giver adgang til SIS for administrative myndigheder med henblik på at forebygge og bekæmpe kriminalitet (handel med stjålne køretøjer). Behovet for en stærk begrundelse og et solidt retsgrundlag for adgang til SIS II er præciseret i punkt 4.2.2. i denne udtalelse.

Den Europæiske Tilsynsførende for Databeskyttelse henviser til de bemærkninger i denne forbindelse, som Den Fælles Tilsynsmyndighed for Schengen fremsætter i sin udtalelse om det foreslåede retsgrundlag for SIS II. Især Den Fælles Tilsynsmyndigheds forslag om at ændre den foreslåede afgørelse, således at den omfatter denne adgang, skal følges.

5. **KOMMISSIONENS OG MEDLEMSSTATERNES ROLLE**

En klar beskrivelse og ansvarsfordeling i forbindelse med SIS II er altafgørende, ikke blot med henblik på at systemet kan fungere smidigt, men også set ud fra et tilsynssynspunkt. Fordelingen af tilsynsbeføjelserne vil følge af beskrivelsen af ansvarsområderne, derfor er der behov for absolut klarhed.

5.1. **Kommissionens rolle**

Den Europæiske Tilsynsførende for Databeskyttelse er meget tilfreds med kapitel III i begge forslag, som beskriver Kommissionens rolle og ansvar i forbindelse med SIS II (»operationel forvaltning«). Denne forklaring findes ikke i VIS-forslaget. Dette kapitel giver imidlertid ikke en udtømmende forklaring på Kommissionens rolle. Som anført i kapitel 9 i denne udtalelse er Kommissionen også involveret i gennemførelsen og forvaltningen af systemet gennem komitologiproceduren.

Med hensyn til databeskyttelse har Kommissionen en rolle, som allerede er anerkendt i VIS- og Eurodac-systemerne, nemlig som ansvarlig for den operationelle forvaltning. Kombineret med dens store rolle i forbindelse med udviklingen og opretholdelsen af systemet, skal denne ses som en rolle som sui generis-registeransvarlig. Dette er som allerede sagt i udtalelsen fra Den Europæiske Tilsynsførende for Databeskyttelse om VIS meget mere end en registerfører, men også mere begrænset end en normal registeransvarlig, da Kommissionen ikke har nogen adgang til de data, der behandles i SIS II.

Da SIS II vil bygge på komplekse systemer, hvoraf nogle afhænger af nye teknologier, insisterer Den Europæiske Tilsynsførende for Databeskyttelse på at styrke Kommissionens ansvar for at holde systemerne ajour ved at gennemføre den bedste tilgængelige teknologi vedrørende sikkerhed og databeskyttelse.

Det skal derfor tilføjes i artikel 12 i forslagene, at Kommissionen regelmæssigt skal foreslå, at der gennemføres nye teknologier, som udgør det aktuelle tekniske niveau på dette område og som vil forbedre databeskyttelses- og sikkerhedsniveauerne samt lette arbejdet for de nationale myndigheder, der har adgang til disse oplysninger.

5.2. **Medlemsstaternes rolle**

Medlemsstaternes situation er ikke rigtig klar, da det er temmelig vanskeligt at vide, hvilke(n) myndighed(er), der skal være de(n) registeransvarlige.

Forslagene beskriver en rolle for det nationale SIS II-kontor (at sikre de kompetente myndigheders adgang til SIS II) samt for Sirene-myndighederne (at sikre udvekslingen af alle supplerende oplysninger). Medlemsstaterne skal også varetage deres NS's (»nationale systems«) funktion og sikkerhed. Det står ikke klart, om dette sidstnævnte ansvar skal varetages af en af ovennævnte myndigheder. Der er under alle omstændigheder brug for en afklaring.

Med hensyn til databeskyttelse skal Kommissionen og medlemsstaterne betragtes som fælles registeransvarlige, der hver har specifikke ansvarsområder. Den eneste måde at sikre, at der føres tilsyn med alle områder af SIS II-aktiviteterne, er at anerkende eksistensen af disse supplerende opgaver.

6. **DE REGISTREREDES RETTIGHEDER**

6.1. **Information**

6.1.1. *Den foreslåede forordning*

Artikel 28 i den foreslåede forordning forudser, at den registrerede har ret til at blive informeret, hovedsagelig som følge af artikel 10 i direktiv 95/46. Dette er en velkommen forandring sammenlignet med den nuværende situation, hvor konventionen ikke indeholder en udtrykkelig ret til oplysninger. Der er imidlertid mulighed for forbedringer på følgende punkter.

Der skal tilføjes nogle oplysninger på listen, da det vil bidrage til at sikre en retfærdig behandling af den registrerede ([1]). Disse oplysninger skal vedrøre tidsrummet for bevaring af oplysningerne, eksistensen af retten til at anmode om genbehandling eller appel af beslutningen om at foretage en indberetning (se i nogle tilfælde artikel 15, stk. 3, i den foreslåede forordning), muligheden for at få bistand fra databeskyttelsesmyndigheden og eksistensen af klageadgang.

Der anføres ikke i den foreslåede forordning noget tidspunkt for, hvornår oplysningerne skal gives. Dette kan gøre det umuligt at udøve den registreredes rettigheder. For at gøre disse rettigheder effektive burde forordningen fastsætte et præcist tidspunkt, hvor oplysningerne skal gives, alt efter hvilken myndighed, der har foretaget indberetningen.

En praktisk løsning ville være at indsætte oplysninger om indberetningen i den afgørelse, som ligger til grund for indberetningen: enten en retlig eller en administrativ afgørelse, der er baseret på en trussel mod den offentlige orden (…) eller en afgørelse om tilbagesendelse eller udsendelse ledsaget af et forbud mod fornyet indrejse. Dette bør indsættes i artikel 28 i forordningen.

6.1.2. *Den foreslåede afgørelse*

Artikel 50 i afgørelsen fastsætter, at den registrerede kan anmode om oplysninger og angiver de mulige grunde til at nægte at give disse oplysninger. Begrænsningerne i denne ret er lette at forstå i betragtning af arten af dataene og den kontekst, hvori de behandles.

Retten til oplysninger skal imidlertid ikke være betinget af, at den registrerede anmoder herom (dette ville faktisk snarere være definitionen på en anmodning om adgang). Man kan formode, at behovet for at »anmode om« oplysninger er berettiget i tilfælde, hvor den registrerede ikke kan informeres, fordi han ikke er fundet.

Det ville være bedre at tilføje en undtagelse fra retten til oplysninger i tilfælde, hvor det viser sig at være umuligt eller uforholdsmæssigt vanskeligt at give denne information. Artikel 50 i afgørelsen skal ændres tilsvarende.

([1]) Se udtalelsen fra Den Europæiske Tilsynsførende for Databeskyttelse om visuminformationssystemet, punkt 3.10.1.

Denne løsning vil også være i overensstemmelse med anvendelsen af udkastet til rammeafgørelse om databeskyttelse i tredje søjle.

6.2. **Adgang**

Både den foreslåede forordning og den foreslåede afgørelse indeholder frister for at besvare anmodningerne om adgang, hvilket er en positiv udvikling. Da proceduren for udøvelse af adgangsretten imidlertid er fastlagt på nationalt plan, kan man undre sig over, hvordan de frister, der er fastsat i forslagene, kan overholdes med de eksisterende procedurer, især hvis medlemsstaterne har kortere frister til at besvare en anmodning om adgang. Det bør gøres klart, at de frister, som er de mest gunstige for den registrerede, skal anvendes.

6.2.1. *Den foreslåede forordning*

Det er værd at notere, at de restriktioner i adgangsretten (»nægtes adgang til oplysningerne, hvis det kan skade gennemførelsen af den lovlige foranstaltning, der følger af indberetningen, eller til beskyttelse af tredjemands rettigheder og frihedsrettigheder«), der for øjeblikket findes i Schengenkonventionen, ikke er medtaget i den foreslåede forordning.

Dette skyldes formentlig anvendelsen af direktiv 95/46/EF, som giver mulighed for at gennemføre undtagelser i de nationale lovgivninger (artikel 13). Det bør under alle omstændigheder understreges, at anvendelsen af artikel 13 i den nationale lovgivning til begrænsning af adgangsretten altid skal ske i overensstemmelse med artikel 8 i EMRK og kun i begrænsede tilfælde.

6.2.2. *Den foreslåede afgørelse*

Den foreslåede afgørelse tager begrænsningen af adgangsretten op ligesom i Schengen-konventionen. Den foreslåede rammeafgørelse indeholder i det væsentlige de samme begrænsninger i adgangsretten, så vedtagelsen af dette instrument vil ikke gøre nogen særlig forskel i denne henseende.

Da adgangen til retshåndhævelsesdata i flere medlemsstater er »indirekte« (hvilket betyder, at den udøves via den nationale databeskyttelsesmyndighed), ville det være nyttigt med en bestemmelse om, at databeskyttelsesmyndighederne har pligt til at samarbejde aktivt om udøvelsen af adgangsretten.

6.3. **Retten til genbehandling eller appel af afgørelsen om at foretage en indberetning**

Artikel 15, stk. 3, i forordningen indfører en ret til at få sagen genbehandlet af eller til at appellere afgørelsen til en retsmyndighed for så vidt angår afgørelsen om at foretage en indberetning, når afgørelsen træffes af en administrativ myndighed. Dette er en velkommen tilføjelse i forhold til den nuværende Schengen-konvention.

Dette understreger behovet for fuldstændig og rettidig information af den registrerede som nævnt i punkt 6.1 ovenfor, ellers forbliver denne nye ret teoretisk.

6.4. **Klageadgang**

Artikel 30 i den foreslåede forordning og artikel 52 i den foreslåede afgørelse giver ret til at indbringe en sag for eller klage til retten i en medlemsstat, hvis den registrerede nægtes ret til at få adgang til eller ret til at ændre eller slette data eller ret til at opnå oplysninger eller erstatning.

Ordene (»enhver, der befinder sig på en medlemsstats område«) antyder, at klageren skal være fysisk til stede på området for at indbringe sin sag for retten. Denne territoriale begrænsning er ikke berettiget og kan gøre klageadgangen ineffektiv, da klageren meget ofte vil indbringe en sag, netop fordi han ikke har adgang til Schengen-området. Da direktivet desuden er *lex generalis* i forhold til den foreslåede forordning, skal artikel 22 i direktivet tages med i betragtning; den fastsætter, at »enhver« har ret til at indbringe en klage uanset bopæl. Den foreslåede rammeafgørelse indeholder heller ikke nogen territorial begrænsning. Den Europæiske Tilsynsførende for Databeskyttelse foreslår, at den territoriale begrænsning i artikel 30 og 52 udelades.

7. **TILSYN**

7.1. **Indledende bemærkninger: fælles ansvar**

Forslagene fordeler tilsynsopgaverne mellem de nationale tilsynsmyndigheder ([1]) og Den Europæiske Tilsynsførende for Databeskyttelse på deres respektive ansvarsområder. Dette er i overensstemmelse med forslagenes tilgang til gældende lovgivning og ansvaret for SIS II's funktion og anvendelse og med behovet for et effektivt tilsyn.

Den Europæiske Tilsynsførende for Databeskyttelse ser med tilfredshed på denne tilgang, som den fremgår af artikel 31 i den foreslåede forordning og artikel 53 i den foreslåede afgørelse. Med henblik på bedre at forstå og at præcisere de respektive opgaver foreslår Den Europæiske Tilsynsførende for Databeskyttelse imidlertid, at hver artikel opdeles i flere bestemmelser, der hver vedrører et niveau af tilsynet, som det så rigtigt er gjort i VIS-forslaget.

([1]) Tilsynsmyndighederne for Europol og Eurojust er også involveret, men i mindre omfang.

7.2. **Tilsyn foretaget af de nationale databeskyttelsesmyndigheder**

I henhold til artikel 31 i den foreslåede forordning og artikel 53 i den foreslåede afgørelse skal hver enkelt medlemsstat sikre, at en uafhængig myndighed fører tilsyn med, at behandlingen af SIS II-personoplysninger sker i overensstemmelse med loven.

Artikel 53 i den foreslåede afgørelse tilføjer en ret for fysiske personer til at anmode tilsynsmyndigheden om at kontrollere, at behandlingen af oplysninger vedrørende den pågældende er lovlig. Der er ikke indsat en tilsvarende bestemmelse i den foreslåede forordning, da direktivet finder anvendelse som *lex generalis*. Man må derfor gå ud fra, at de nationale databeskyttelsesmyndigheder med hensyn til SIS II kan udøve alle de beføjelser, som tildeles dem med artikel 28 i direktiv 95/46/EF, herunder at kontrollere at databehandling er lovlig. Artikel 31, stk. 1, i forordningen præciserer deres opgaver, men kan ikke udgøre en begrænsning af disse beføjelser. Det bør klart angives i teksten til den foreslåede forordning, at disse beføjelser anerkendes.

Med hensyn til den foreslåede afgørelse giver den mere omfattende opgaver til de nationale tilsynsmyndigheder, fordi dens *lex generalis* er en anden. En situation, hvor tilsynsmyndighederne har forskellige opgaver og beføjelser alt efter kategorien af behandlede data er imidlertid ikke forsvarlig og meget vanskelig at forvalte i praksis. En sådan må derfor undgås, enten ved at tildele disse myndigheder samme beføjelser i selve teksten til den foreslåede afgørelse eller ved at henvise til en anden *lex generalis* (nemlig rammeafgørelsen om databeskyttelse i tredje søjle), der giver databeskyttelsesmyndighederne flere beføjelser.

7.3. **Tilsyn foretaget af Den Europæiske Tilsynsførende for Databeskyttelse**

Den Europæiske Tilsynsførende for Databeskyttelse overvåger, at Kommissionens databehandlingsaktiviteter udføres i overensstemmelse med forslagene. På samme måde skal Den Europæiske Tilsynsførende for Databeskyttelse kunne udøve alle sine beføjelser i henhold til forordning 45/2001, dog under hensyn til Kommissionens begrænsede beføjelser med hensyn til selve dataene.

Det er nyttigt at tilføje, at Den Europæiske Tilsynsførende for Databeskyttelse ifølge artikel 46, litra f), i forordning 45/2001 »har til opgave at samarbejde med de nationale tilsynsmyndigheder i det omfang, det er nødvendigt for udførelsen af deres respektive pligter«. Samarbejdet med medlemsstaterne om tilsynet med SIS II stammer ikke kun fra forslagene, men også fra forordning 45/2001.

7.4. **Fælles tilsyn**

Forslagene anerkender også behovet for at samordne de forskellige involverede myndigheders tilsynsaktiviteter. Artikel 31 i den foreslåede forordning og artikel 53 i den foreslåede afgørelse fastsætter, at »De nationale tilsynsmyndigheder og Den Europæiske Tilsynsførende for Databeskyttelse samarbejder aktivt med hinanden. Den Europæiske Tilsynsførende for Databeskyttelse indkalder mindst én gang om året til et møde med henblik herpå.«

Den Europæiske Tilsynsførende for Databeskyttelse glæder sig over dette forslag, som i det væsentligste indeholder de nødvendige elementer til at skabe samarbejdet — som virkeligt er afgørende — mellem de myndigheder, der har ansvaret for tilsynet på nationalt og europæisk plan. Det understreges, at forslagene kræver et møde mindst én gang om året, men at dette skal betragtes som et minimum.

Det ville imidlertid være bedre, hvis disse bestemmelser (artikel 31 i den foreslåede forordning og artikel 53 i den foreslåede afgørelse) blev gjort klarere for så vidt angår indholdet af denne samordning. Den nuværende Fælles Tilsynsmyndighed har kompetence til at undersøge vanskeligheder med fortolkningen eller anvendelsen af konventionen, til at undersøge problemer, der måtte opstå med udøvelsen af et uafhængigt tilsyn eller retten til adgang, og til at udarbejde harmoniserede forslag til fælles løsninger på eksisterende problemer.

De nye forslag må ikke føre til en svækkelse af det fælles tilsyns nuværende rækkevidde. Hvis det er klart, at databeskyttelsesmyndighederne med hensyn til SIS II kan udøve alle de tilsynsbeføjelser, som de tildeles med direktivet, kan disse myndigheders samarbejde omfatte brede aspekter af tilsynet med SIS II, herunder den nuværende Fælles Tilsynsmyndigheds opgaver som angivet i artikel 115 i Schengen-konventionen.

For at gøre dette fuldstændig klart vil det imidlertid være nyttigt at anføre det udtrykkeligt i forslagene.

8. SIKKERHED

Forvaltning og opretholdelse af et optimalt sikkerhedsniveau for SIS II er en grundlæggende forudsætning for, at der kan sikres en passende beskyttelse af de personoplysninger, der lagres i databasen. For at opnå et sådant tilfredsstillende beskyttelsesniveau må der gennemføres passende garantier for behandling af de potentielle risici ved systemets infrastruktur og de berørte personer. Dette spørgsmål omhandles i øjeblikket i forskellige dele af forslaget, men der bør foretages nogle forbedringer.

Artikel 10 og 13 i forslaget indeholder forskellige foranstaltninger vedrørende datasikkerhed og angiver de former for misbrug, der skal forebygges. Den Europæiske Tilsynsførende for Databeskyttelse glæder sig over, at der er indsat bestemmelser om systematisk (selv)revision af sikkerhedsforanstaltninger i disse artikler.

Artikel 59 i den foreslåede afgørelse og artikel 34 i den foreslåede forordning, der indeholder bestemmelser om overvågning og evaluering, bør imidlertid ikke kun omfatte aspekter som resultater, omkostningseffektivitet og tjenesternes kvalitet, men også opfyldelse af retlige krav, især inden for databeskyttelse. Den Europæiske Tilsynsførende for Databeskyttelse henstiller derfor, at disse artiklers anvendelsesområde udvides til overvågning og rapportering om behandlingens lovlighed.

Som supplement til artikel 10, stk. 1, litra f), eller artikel 18 i den foreslåede afgørelse og artikel 17 i den foreslåede forordning vedrørende de behørigt autoriserede personer, der har adgang til oplysningerne, bør det desuden tilføjes, at medlemsstaterne (samt Europol og Eurojust) skal sikre, at der findes præcise brugerprofiler (som skal stilles til rådighed for de nationale tilsynsmyndigheder med henblik på kontrol). Ud over disse brugerprofiler skal der udarbejdes en fuldstændig liste over brugeridentiteter, som medlemsstaterne permanent skal holde ajour. Det samme gælder *mutatis mutandis* for Kommissionen.

Disse sikkerhedsforanstaltninger er suppleret med overvågnings- og organisationsmæssige garantier. Artikel 14 i forslagene beskriver betingelserne for og årsagerne til, at der skal føres registre over alle databehandlingsoperationer. Disse registre skal ikke kun føres for at overvåge databeskyttelsen og sikre datasikkerheden, men også for at konsolidere den regelmæssige selvrevision af SIS II, som kræves i artikel 10. Selvrevisionsrapporterne vil bidrage til en effektiv udførelse af tilsynsmyndighedernes opgaver, idet disse vil kunne identificere de svageste punkter og fokusere på dem under deres egen revisionsprocedure.

Som det er anført tidligere i denne udtalelse skal der være en nøje begrundelse for at tildele flere adgangspunkter til systemet, da det automatisk øger risikoen for misbrug. Der bør derfor i artikel 4, stk. 1, litra b), i forslagene kræves en konkret påvisning af, at der er behov for mere end et adgangspunkt.

Forslagene forklarer ikke klart behovet for nationale kopier af det centrale system og giver anledning til alvorlige betænkeligheder med hensyn til den samlede risiko og sikkerhed ved systemet som f.eks.:

— Flere kopier øger risikoen for misbrug (især i betragtning af de nye oplysninger som f.eks. biometriske data)

— De oplysninger, der er berørt af disse kopier, er ikke veldefinerede

— Kravene om nøjagtighed, kvalitet og tilgængelighed i artikel 9 udgør store tekniske udfordringer og øger derfor omkostningerne alt efter det aktuelle tekniske niveau

— De nationale myndigheders overvågning af disse kopier vil kræve yderligere menneskelige og finansielle ressourcer, som måske ikke altid vil være til rådighed.

Under hensyn til risikoen er Den Europæiske Tilsynsførende for Databeskyttelse hverken overbevist om nødvendigheden af (i betragtning af den tilgængelige teknologi) eller fordelen ved at anvende nationale kopier. Han anbefaler, at medlemsstaternes mulighed for at anvende nationale kopier udelades.

Hvis der skal udvikles nationale kopier, minder Den Europæiske Tilsynsførende for Databeskyttelse om, at princippet om formålsbegrænsning skal overholdes strengt i forbindelse med anvendelse nationalt. Der må heller aldrig søges i den nationale kopi på andre måder end i den centrale database.

Lovligheden af behandlingen af personoplysninger er baseret på nøje respekt for datasikkerhed og dataintegritet. Den Europæiske Tilsynsførende for Databeskyttelse vil føre et effektivt tilsyn med disse processer og kan ikke kun overvåge datasikkerheden, men må også overvåge integriteten gennem en analyse af de logs, der er til rådighed. Det er således nødvendigt at tilføje »dataintegritet« i artikel 14, stk. 6.

9. **UDVALGSPROCEDURER**

Forslagene omtaler udvalgsprocedurer i flere tilfælde, hvor der kræves teknologiske afgørelser om gennemførelsen eller forvaltningen af SIS II. Som det er anført i VIS-udtalelsen af tilsvarende årsager vil disse afgørelser have en betydelig indflydelse på den korrekte gennemførelse af principperne om formål og proportionalitet.

Den Europæiske Tilsynsførende for Databeskyttelse tilråder, at afgørelser med en væsentlig indvirkning på databeskyttelsen som f.eks. adgang til og indsættelse af data, udveksling af supplerende oplysninger, datakvalitet og indberetningers kompatibilitet, overholdelse af tekniske krav til nationale kopier osv. skal træffes i form af en forordning eller et direktiv, helst efter den fælles beslutningsprocedure. ([1])

([1]) Se også Den Europæiske Tilsynsførende for Databeskyttelses udtalelse om visuminformationssystemet, punkt 3.12, og Den Europæiske Tilsynsførende for Databeskyttelses udtalelse om forslaget til direktiv om opbevaring af data der behandles i forbindelse med levering af offentlige elektroniske kommunikationstjenester af 26. september 2005, punkt 60.

I alle andre tilfælde med indvirkning på databeskyttelsen skal Den Europæiske Tilsynsførende for Databeskyttelse have mulighed for at rådgive om de valg, som disse udvalg har foretaget.

Den Europæiske Tilsynsførende for Databeskyttelses rådgivende rolle bør omtales i artikel 60 og 61 i afgørelsen og artikel 35 i forordningen.

I det mere specifikke tilfælde med de tekniske regler for sammenkobling af indberetninger (artikel 26 i forordningen og artikel 46 i afgørelsen), må det forklares, at der er behov for en anden komitologifunktion (rådgivende funktion for afgørelsen og forskriftsmæssig funktion for forordningen).

10. **INTEROPERABILITET**

Da Kommissionens meddelelse om de kommende EU-systemers interoperabilitet endnu ikke foreligger, er det vanskeligt korrekt at vurdere fordelen ved de påtænkte, men endnu ikke fastlagte synergier.

I denne forbindelse henviser Den Europæiske Tilsynsførende for Databeskyttelse også til Rådets erklæring af 25. marts 2004 om bekæmpelse af terrorisme, hvori Kommissionen anmodes om at forelægge forslag til forbedring af interoperabilitet og synergier mellem informationssystemerne (SIS, VIS og Eurodac). Han henviser også til de igangværende drøftelser om, hvilket organ der i fremtiden vil kunne få overdraget opgaven med at forvalte de forskellige store systemer (jf. også punkt 3.8 i denne udtalelse).

Som Den Europæiske Tilsynsførende for Databeskyttelse allerede anførte i sin udtalelse om visuminformationssystemet er interoperabilitet en kritisk og afgørende forudsætning for effektiviteten i store edb-systemer som SIS II. Den gør det muligt at begrænse de samlede udgifter på en sammenhængende måde og undgå naturlige overlapninger af heterogene elementer.

— Interoperabilitet kan også bidrage til målsætningen om at opretholde et højt sikkerhedsniveau inden for et område uden intern grænsekontrol mellem medlemsstaterne ved at anvende den samme proceduremæssige standard på alle de elementer, der indgår i denne politik. Det er imidlertid afgørende, at der sondres mellem to interoperabilitetsniveauer:

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

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

Af de tilgængelige beskyttelsesforanstaltninger, der anvendes til at begrænse systemets formål og forebygge »funktionsskred«, er anvendelsen af forskellige teknologistandarder en af dem, der kan bidrage til denne begrænsning. Desuden bør enhver form for interaktion mellem to forskellige systemer være veldokumenteret. Interoperabilitet må aldrig føre til en situation, hvor en myndighed, der ikke har ret til at få indsigt i eller anvende visse oplysninger, kan skaffe sig adgang til dem gennem et andet informationssystem. Efter læsning af forslagene ser det for eksempel ud til, at der ikke vil være et automatisk fingeraftryksidentifikationssystem (AFIS) i de første år af SIS II, idet der kun henvises til en fremtidig biometrisk søgemaskine. Hvis det påtænkes at indføre et scenario, hvor AFIS fra andre EU-systemer anvendes, bør dette dokumenteres klart med de nødvendige garantier for sådanne synergier.

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

11. **KONKLUSIONER**

11.1. **Generelle bemærkninger**

1. Den Europæiske Tilsynsførende for Databeskyttelse ser med tilfredshed på flere positive aspekter ved disse forslag, som på nogle punkter udgør en forbedring i forhold til den nuværende situation. Han erkender, at bestemmelserne om databeskyttelse generelt er udarbejdet meget omhyggeligt.

2. Den Europæiske Tilsynsførende for Databeskyttelse understreger, at den nye retlige ordning, uanset hvor kompleks den er, skal

   — sikre et højt databeskyttelsesniveau

   — være forudsigelig for borgerne samt for de myndigheder, der udveksler oplysninger

   — anvendes ensartet i forskellige kontekster (første eller tredje søjle).

3. Desuden skal tilføjelserne af nye elementer i SIS II, der øger dets eventuelle indvirkning på personers liv, ledsages af strengere garantier, som er beskrevet i udtalelsen, især følgende:

— Der kan ikke gives nye myndigheder adgang til SIS II-data uden en meget vægtig begrundelse. Adgangen skal også begrænses så meget som muligt, både med hensyn til tilgængelige oplysninger og autoriserede personer.

— Sammenkobling af indberetninger kan aldrig, selv ikke indirekte, medføre en ændring i adgangsrettighederne.

— Ikke-vedtaget lovgivning kan ikke betragtes som et gyldigt grundlag for at indsætte oplysninger i SIS II (indberetninger med henblik på indrejseforbud).

— Retsgrundlaget for adgangen for de myndigheder, der har ansvaret for udstedelse af køretøjsregistreringsattester, skal tages op til overvejelse, da den hovedsagelig tager sigte på kriminalitetsbekæmpelse.

— Den Europæiske Tilsynsførende for Databeskyttelse erkender, at anvendelsen af biometriske oplysninger kan forbedre systemets resultater og hjælpe ofre for identitetstyveri. Virkningen af denne fornyelse synes imidlertid ikke at være tilstrækkelig gennemtænkt, og disse datas pålidelighed synes at være overdrevet.

11.2 **Særlige bemærkninger**

1. Den Europæiske Tilsynsførende for Databeskyttelse er glad for, at Kommissionen erkender, at forordning 45/2001 finder anvendelse på alle Kommissionens databehandlingsaktiviteter inden for SIS II, da denne vil bidrage til at sikre en konsekvent og ensartet anvendelse af reglerne om beskyttelse af personers grundlæggende rettigheder og frihedsrettigheder med hensyn til behandling af personoplysninger.

2. For at sikre en streng formålsbegrænsning på nationalt plan anbefaler Den Europæiske Tilsynsførende for Databeskyttelse, at der i SIS II-forslagene (artikel 21 i den foreslåede forordning og artikel 40 i den foreslåede afgørelse) indsættes en bestemmelse med samme virkning som den nuværende artikel 102, stk. 4, i Schengen-konventionen, der begrænser medlemsstaternes mulighed for at anvende oplysninger på måder, der ikke forekommer i SIS II-teksterne.

3. Der bør gælde strenge betingelser for at få adgang til SIS II-oplysninger for enhver myndighed:

— Adgangen skal være forenelig med det generelle formål med SIS II og i overensstemmelse med retsgrundlaget.

— Det skal bevises, at der er behov for adgang til SIS II-oplysninger.

— Det skal fastlægges udtrykkeligt og restriktivt, hvilken brug der vil blive gjort af dataene

— Betingelserne for adgangen skal være veldefinerede og begrænsede. Der skal især foreligge en ajourført liste over de personer, der har adgang til SIS II, også for Europol og Eurojust.

— Det forhold, at disse myndigheder får adgang til SIS II-oplysninger, kan aldrig være en begrundelse for at indsætte eller bevare oplysninger i systemet, hvis de ikke er til nytte i forbindelse med den bestemte indberetning, som de er en del af.

— Tidsrummet for bevaring af dataene kan ikke forlænges, hvis det ikke er nødvendigt for formålet med indsættelsen af oplysningerne.

4. I det særlige tilfælde med Europol og Eurojust anmoder Den Europæiske Tilsynsførende for Databeskyttelse indtrængende Kommissionen om restriktivt at fastlægge de opgaver, til hvis udførelse det vil være berettiget at give adgang. Europols og Eurojusts adgang skal desuden være begrænset til oplysninger om personer, hvis navne allerede findes i deres filer. Det foreslås også, at der kun gives Europol og Eurojust ét adgangspunkt.

5. Med hensyn til indberetningerne med henblik på indrejseforbud bør de bestemmelser, der er baseret på lovgivning, som endnu ikke er vedtaget, enten trækkes tilbage eller omredigeres på en måde — baseret på eksisterende lovgivning — der gør det muligt for borgerne at vide, præcis hvilke foranstaltninger myndighederne kan træffe over for dem.

6. Tidsrummene for bevaring af oplysningerne er blevet forlænget, uden at der gives nogen seriøs begrundelse herfor. Hvis der ikke er nogen overbevisende begrundelse, bør de afkortes til deres nuværende varighed, især i tilfælde af indberetninger med henblik på diskret overvågning eller særlig kontrol.

7. Kommissionens rolle er beskrevet således, at den er ansvarlig for den operationelle forvaltning. Kombineret med dens store rolle i forbindelse med udviklingen og opretholdelsen af systemet bør denne ses som en rolle som sui generis-registeransvarlig. Dette er meget mere end en registerfører, men også mere begrænset end en normal registeransvarlig, da Kommissionen ikke har adgang til de data, der behandles i SIS II.

   Det bør i forbindelse med denne rolle tilføjes i artikel 12 i begge forslag, at Kommissionen regelmæssigt skal foreslå, at der gennemføres nye teknologier, som udgør det aktuelle tekniske niveau på dette område og som vil forbedre databeskyttelses- og sikkerhedsniveauerne.

8. Med hensyn til medlemsstaternes rolle er der behov for en præcisering af, hvilke myndigheder der er de registeransvarlige.

9. Med hensyn til information af den registrerede:

   — bør der i den foreslåede forordning tilføjes nogle oplysninger på listen: tidsrummet for bevaring af oplysningerne, eksistensen af retten til at anmode om genbehandling eller appel af beslutningen om at foretage en indberetning, muligheden for at få bistand fra databeskyttelsesmyndigheden og eksistensen af klageadgang.

     Desuden skal der med hensyn til det tidspunkt, hvor disse oplysninger gives, være pligt til at give oplysninger om indberetningen i den afgørelse, der ligger til grund for indberetningen.

   — bør artikel 50 i den foreslåede afgørelse ændres, således at retten til oplysninger ikke er betinget af, at den registrerede anmoder herom.

10. Med hensyn til fristerne for besvarelse af en anmodning om adgang er fastsættelsen af frister i forslagene en god ting. Når de nationale lovgivninger også fastsætter frister, bør det gøres klart, at de frister, som er mest gunstige for den registrerede, skal anvendes.

    Det vil desuden være nyttigt med en bestemmelse om, at databeskyttelsesmyndighederne har pligt til at samarbejde aktivt om udøvelsen af adgangsretten.

11. Med hensyn til klageadgang foreslår Den Europæiske Tilsynsførende for Databeskyttelse, at den territoriale begrænsning i artikel 30 og 52 udelades.

12. Med hensyn til de nationale databeskyttelsesmyndigheders beføjelser:

   — i forordningen: det må overvejes, om de i forbindelse med SIS II kan udøve alle de beføjelser, som de får i artikel 28 i direktiv 95/46/EF; dette bør gøres klart i teksten til den foreslåede forordning.

   — i den foreslåede afgørelse: tilsynsmyndighederne bør have de samme beføjelser som i forordningen/direktivet.

13. Med hensyn til Den Europæiske Tilsynsførende for Databeskyttelses beføjelser: Den Europæiske Tilsynsførende for Databeskyttelse bør kunne udøve alle sine beføjelser i henhold til forordning 45/2001, dog under hensyn til Kommissionens begrænsede beføjelser med hensyn til selve oplysningerne.

14. Med hensyn til samordnet tilsyn: det anerkendes også i forslagene, at der er behov for at samordne de forskellige involverede myndigheders tilsynsaktiviteter. Den Europæiske Tilsynsførende for Databeskyttelse udtrykker tilfredshed med, at de i det væsentligste indeholder de elementer, der er nødvendige for at skabe samarbejde mellem de myndigheder, der har ansvaret for tilsynet på nationalt og europæisk plan. Disse bestemmelser (artikel 31 i den foreslåede forordning og artikel 53 i den foreslåede afgørelse) burde dog præciseres nærmere for så vidt angår indholdet af denne samordning.

15. Artikel 10 og 13 i forslaget indeholder forskellige foranstaltninger med henblik på datasikkerhed; medtagelsen af bestemmelser om systematisk (selv)revision af sikkerhedsforanstaltninger er hensigtsmæssig.

   — Artikel 59 i den foreslåede afgørelse og artikel 34 i den foreslåede forordning, der indeholder bestemmelser om overvågning og evaluering, skal imidlertid ikke kun omfatte aspekter som resultater, omkostningseffektivitet og tjenesternes kvalitet, men også opfyldelse af retlige krav, især inden for databeskyttelse. Disse bestemmelser skal ændres tilsvarende.

   — Det bør desuden som supplement til artikel 10, stk. 1, litra f), eller artikel 18 i den foreslåede afgørelse og artikel 17 i den foreslåede forordning tilføjes, at medlemsstaterne, Europol og Eurojust bør sikre, at der findes præcise brugerprofiler (som bør stilles til rådighed for de nationale tilsynsmyndigheder med henblik på kontrol). Ud over disse brugerprofiler skal der udarbejdes en fuldstændig liste over brugeridentiteter, som medlemsstaterne permanent skal holde ajour. Det samme gælder for Kommissionen.

   — Lovligheden af behandlingen af personoplysninger er baseret på nøje respekt for datasikkerhed og dataintegritet. Den Europæiske Tilsynsførende for Databeskyttelse bør kunne overvåge ikke blot datasikkerheden, men også dataenes integritet gennem en analyse af de logs, der er til rådighed. Det er således nødvendigt at tilføje »dataintegritet« i artikel 14, stk. 6.

16. Anvendelsen af nationale kopier kan medføre mange yderligere risici. Den Europæiske Tilsynsførende for Databeskyttelse er hverken overbevist om nødvendigheden af (i betragtning af den tilgængelige teknologi) eller fordelen ved at anvende nationale kopier. Han anbefaler, at man udelader eller i det mindste alvorligt begrænser medlemsstaternes mulighed for at anvende nationale kopier. Hvis der alligevel udvikles nationale kopier, minder Den Europæiske Tilsynsførende for Databeskyttelse om, at princippet om formålsbegrænsning skal overholdes strengt i forbindelse med den nationale brug. Der må heller aldrig søges i den nationale kopi på andre måder end i den centrale database.

17. Udvalgsprocedurer: afgørelser med en væsentlig indvirkning på databeskyttelsen bør træffes i form af en forordning eller et direktiv, helst efter den fælles beslutningsprocedure. Hvis udvalgsproceduren faktisk anvendes, bør Europæiske Tilsynsførende for Databeskyttelses rådgivende rolle omtales i artikel 60 og 61 i afgørelsen og artikel 35 i forordningen.

18. Interoperabilitet mellem systemerne må ikke gennemføres, hvis det krænker princippet om begrænsning af formålet, og ethvert forslag herom bør forelægges Den Europæiske Tilsynsførende for Databeskyttelse.

Udfærdiget i Bruxelles den 19. oktober 2005,

Peter HUSTINX

Den Europæiske Tilsynsførende for Databeskyttelse