

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE

Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om forslaget til Rådets afgørelse om adgang til søgning i visuminformationssystemet (VIS) for de myndigheder i medlemsstaterne, der har ansvaret for den indre sikkerhed, og for Europol med henblik på forebyggelse, afsløring og efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger (KOM (2005) 600 endelig)

(2006/C 97/03)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE
HAR —

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

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

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

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

under henvisning til Kommissionens anmodning, modtaget den 29. november 2005, om en udtalelse i overensstemmelse med artikel 28, stk. 2, i forordning (EF) nr. 45/2001 —

VEDTAGET FØLGENDE UDTALELSE:

1. INDLEDNING

1.1. Indledende bemærkninger

Forslaget til Rådets afgørelse om adgang til søgning i visuminformationssystemet (VIS) for de myndigheder i medlemsstaterne, der har ansvaret for den indre sikkerhed, og for Europol med henblik på forebyggelse, afsløring og efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger (i det følgende benævnt »forslaget«) blev af Rådet forelagt Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) ved skrivelse af 24. november 2005. EDPS fortolker denne skrivelse som en

anmodning om at rådgive Fællesskabsinstitutionerne og -organerne som fastsat i artikel 28, stk. 2, i forordning (EF) nr. 45/2001. Efter EDPS's opfattelse bør nærværende udtalelse omtales i præambelen til afgørelsen.

EDPS anser det for vigtigt at afgive en udtalelse om dette følsomme emne, fordi dette forslag er en direkte følge af oprettelsen af VIS, som vil være underlagt hans tilsyn, og hvorom han allerede har afgivet en udtalelse den 23. marts 2005⁽¹⁾. I denne udtalelse blev muligheden af, at retshåndhævende myndigheder får adgang, allerede bragt på bane (se nedenfor); tilkendelse af nye adgangsrettigheder til VIS har for så vidt angår databeskyttelse en afgørende indflydelse på systemet. Det er derfor nødvendigt at afgive en udtalelse om nærværende forslag som opfølgning af den første udtalelse.

1.2. Forslagets betydning

a) Sammenhæng

Det foreliggende forslag er ikke kun vigtigt i sig selv, men også fordi det følger den generelle tendens til at give retshåndhævende myndigheder adgang til adskillige større informations- og identifikationssystemer. Dette er bl.a. nævnt i Kommissionens meddelelse af 24. november 2005 om øget effektivitet, kompatibilitet og synergi blandt europæiske databaser inden for retlige og indre anliggender⁽²⁾, især pkt. 4.6: »I forbindelse med målsætningen om at bekæmpe terrorisme og forbrydelser finder Rådet nu, at de interne sikkerhedsmyndigheders manglende adgang til VIS-data er et problem. Dette samme kan hævdes om samtlige SIS II-data om indvandring og om EURODAC-data«.

Det foreliggende forslag kan derfor ses som en forløber for lignende retsakter udarbejdet i forbindelse med andre databaser, og det er afgørende fra første færd at fastlægge de tilfælde, hvor denne adgang kan tillades.

⁽¹⁾ Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om forslaget til Europa-Parlamentets og Rådets forordning om visuminformationssystemet (VIS) og udveksling af oplysninger mellem medlemsstaterne om visa til kortvarigt ophold (KOM(2004) 835 endelig).

⁽²⁾ KOM (2005) 597 endelig.

b) Følgerne af en ny adgang til VIS

EDPS anerkender helt klart behovet for, at de retshåndhævende myndigheder får de bedst mulige redskaber til identifikation af gerningsmændene til terrorhandlinger og anden alvorlig kriminalitet. Han er også klar over, at VIS-data under visse omstændigheder kan være en væsentlig informationskilde for disse myndigheder.

Det er imidlertid langtfra nogen bagatel at give retshåndhævende organer adgang til første søjle-databaser, uanset hvor berettiget det kan være i bekæmpelsen af terrorisme. Der erindres om, at VIS er et informationssystem udviklet med henblik på den europæiske visumpolitik og ikke som et retshåndhævende instrument. Rutinemæssig adgang ville virkelig betyde en alvorlig krænkelse af princippet om formålsbestemt begrænsning. Det ville medføre et urimeligt indgreb i privatlivets fred for de rejsende, der har samtykket i, at deres data behandles med henblik på at få udstedt et visum, og som forventer, at deres data indsamles, søges og formidles med dette ene formål.

Da informationssystemer er opbygget med et bestemt formål, med garantier, sikkerhed og adgangsbetingelser, der er bestemt af dette formål, ville systematisk adgang med andet formål end det oprindelige ikke kun være en overtrædelse af princippet om formålsbestemt begrænsning, men vil også kunne gøre ovennævnte elementer uhensigtsmæssige eller utilstrækkelige.

I forlængelse heraf kunne en markant ændring af systemet gøre resultaterne af konsekvensvurderingsundersøgelsen ugyldige (som kun omfattede anvendelsen af systemet med det oprindelige formål). Det samme gælder for udtalelserne fra databeskyttelsesmyndighederne. Det vil kunne hævdes, at det nye forslag ændrer præmisserne for deres overensstemmelsesanalyse.

c) Streng begrænsning af denne adgang

På baggrund af ovenstående vil EDPS gerne understrege, at de retshåndhævende myndigheders adgang til VIS kun kan gives under særlige omstændigheder i hvert enkelt tilfælde og skal være ledsaget af strenge garantier. De retshåndhævende myndigheders søgning skal med andre ord ved hensigtsmæssige tekniske og retlige midler være begrænset til specifikke sager.

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

Konkluderende kan de væsentlige krav kort sammenfattes som følger:

- Systematisk adgang bør ikke gives: Det bør i afgørelsen sikres, at tredje søjle-myndighederne altid i hvert enkelt tilfælde undersøger, om adgangen er nødvendig og forholdsmæssig. I denne henseende er en præcis affattelse af retsakten altafgørende, således at der ikke gives mulighed for en bred fortolkning, hvilket igen ville medføre rutinemæssig adgang.
- I de tilfælde, hvor der gives adgang, skal der, i betragtning af denne adgangs følsomme karakter, vedtages passende garantier og betingelser, herunder en omfattende databeskyttelsesordning for anvendelsen af dataene på nationalt plan.

1.3. Indledende bemærkninger

EDPS erkender, at der i det foreslåede dokument er vist databeskyttelsesaspektet meget opmærksomhed, især derved, at adgang begrænses til specifikke tilfælde og kun skal gives som led i bekæmpelse af alvorlig kriminalitet (¹).

Blandt de andre positive elementer skal EDPS også specielt nævne følgende:

- begrænsning til visse former for kriminalitet, jf. Europolkonventionen
- medlemsstaterne har pligt til at udarbejde en liste over de myndigheder, der har adgang, og offentliggøre disse lister
- der skal være et centralt adgangspunkt pr. medlemsstat (og en specialiseret enhed i Europol), således at anmodningerne om adgang bedre kan sorteres og overvåges
- strenge regler for yderligere formidling af data i henhold til forslaget artikel 8, stk. 5
- medlemsstaterne og Europol har pligt til at føre registre over de personer, der har ansvar for datasøgningen.

2. ANALYSE AF FORSLAGET

2.1. Indledende bemærkning

Som forudsætning for at kunne give myndigheder adgang på et tredje søjle-grundlag bør det vigtigste første søjle-VIS-forslag indeholde en passerelle-bestemmelse, der i alt væsentligt bestemmer det eventuelle indhold af en tredje søjle-retsakt som dette forslag. På det tidspunkt, da EDPS afgav sin udtalelse om VIS, var passerelle-bestemmelsen endnu ikke indført, og EDPS havde ikke mulighed for at kommentere den. Alle nedenstående bemærkninger fremsættes derfor med behørigt forbehold for passerelle-bestemmelsens indhold.

(¹) Dette svarer også til Rådets konklusioner fra marts og juli 2005, hvor det kræves, at adgang til VIS for de myndigheder i medlemsstaterne, der har ansvaret for den indre sikkerhed, skal være »betinget af en nøje overholdelse af bestemmelserne om beskyttelse af personoplysninger«.

2.2. Formålet med adgangen

For at sikre en passende begrænsning i adgangen er det vigtigt nøje at fastlægge betingelserne for adgang til VIS. Det er positivt, at det ikke kun af den foreslåede afgørelse selv, men også af begrundelsen og betragtningerne (se navnlig betragtning 7) meget klart fremgår, at der efter hensigten kun skal gives adgang i hvert enkelt tilfælde.

Der kan knyttes en bemærkning til forslaget artikel 5 for således at afstikke fortolkningen af denne.

I artikel 5 begrænses adgangs omfang ved materielle betingelser:

- b) adgangen til søgning skal være nødvendig med henblik på forebyggelse, afsløring eller efterforskning af terrorhandlinger eller andre alvorlige strafbare handlinger
- c) adgangen til søgning skal være nødvendig i et specifikt tilfælde (...) og
- d) der skal på grundlag af konkrete indicier være rimelig grund til at mene, at søgning i VIS-dataene vil bidrage til forebyggelse, afsløring eller efterforskning af en af de pågældende strafbare handlinger.

Disse betingelser er kumulative, idet betingelsen i litra b) mere er en definition af det saglige anvendelsesområde. I praksis betyder det, at den myndighed, der ønsker adgang, skal stå over for en alvorlig strafbar handling som omhandlet i forslaget litra b); der skal være et specifikt tilfælde som omhandlet i litra c). Desuden skal myndigheden kunne påvise, at søgning i VIS-dataene i dette specifikke tilfælde vil bidrage til forebyggelse, afsløring eller efterforskning af den pågældende strafbare handling som fastsat i litra d).

Selv med denne fortolkning af artikel 5 er EDPS betænkelig ved den fleksible affattelse i litra d): »bidrage til« er temmelig bredt. Der er mange tilfælde, hvor VIS-data vil kunne »bidrage til« forebyggelse eller efterforskning af alvorlig kriminalitet. For at begrunde en adgang til VIS-data, der fraviger princippet om formålsbegrænsning, mener EDPS, at denne søgning bør »bidrage væsentligt til« forebyggelse, afsløring eller efterforskning af den pågældende strafbare handling, og foreslår, at artikel 5 ændres i overensstemmelse hermed.

I artikel 10 hedder det, at disse registre skal vise det præcise formål med adgangen. Det »præcise formål« bør omfatte de elementer, der nødvendiggjorde en søgning i VIS som defineret i artikel 5, litra d). Dette ville medvirke til at sikre, at alle søgninger i VIS prøves med henblik på nødvendighed, og mindske risikoen for rutinemæssig adgang.

2.3. Søgekommandoer i VIS-databasen

Artikel 5, stk. 2 og 3, indeholder bestemmelser om adgang i to tempi til VIS-data, idet et sæt data kun er tilgængeligt, hvis der har været et hit på grundlag af det første sæt data. Dette er i sig selv en fornuftig fremgangsmåde. Det første sæt data synes imidlertid at være meget omfattende. Navnlig kan der sættes spørgsmålstejn ved, om data som omhandlet i stk. 5, stk. 2, litra e) og i), er relevante for det første sæt data:

- »Rejsens formål« synes at være en meget generel kommando til effektiv søgning i systemet. Desuden medfører den en risiko for at profilere rejsende på grundlag af dette element
- Med hensyn til »fotografier«: der er kun begrænset mulighed for at søge i så stor en database på grundlag af fotografier; resultaterne af sådanne søgninger opviser på teknologiens nuværende stade uacceptabelt mange forkerte matchende detaljer. Følgerne af en ukorrekt identifikation er meget alvorlig for den pågældende person.

EDPS anmoder derfor om, at dataene i artikel 5, stk. 2, litra e) og i), betragtes som supplerende oplysninger, der er tilgængelige, hvis den første søgning viser, at der allerede er data i systemet, og flyttes til artikel 5, stk. 3.

Som et alternativ kan muligheden for at søge i databasen på grundlag af fotografier gøres til genstand for en teknologisk vurdering i det rådgivende udvalg, så den først indføres, når teknologien er udviklet og kan anses for at være pålidelig nok.

2.4. Anvendelse på medlemsstater, hvor VIS-forordningen ikke finder anvendelse

Myndigheder, der har ansvaret for den indre sikkerhed, fra medlemsstater, der ikke deltager i VIS, kan også få adgang til søgning i VIS. Disse tjenester skal foretage søgningen via en deltagende medlemsstat under behørig overholdelse af betingelserne i artikel 5, stk. 1, litra b) — d) (dvs. i hvert enkelt tilfælde) og indgive en behørigt motiveret skriftlig anmodning.

EDPS vil gerne fremhæve behovet for at få indført visse betingelser for databehandlingen efter søgningen. Ifølge den regel, der gælder for de medlemsstater, der deltager i VIS, skal dataene, så snart de er fundet i VIS, behandles i overensstemmelse med rammeafgørelsen om databeskyttelsen i tredje søjle (se nedenfor). Den samme betingelse bør gælde for de medlemsstater, hvor VIS-forordningen ikke finder anvendelse, men som søger data i VIS. Samme argumenter bør gælde vedrørende føring af registre med henblik på fremtidig kontrol. EDPS anbefaler derfor, at der i forslaget artikel 6 tilføjes et stykke om, at afgørelsens artikel 8 og 10 også gælder for de medlemsstater, hvor VIS-forordningen ikke finder anvendelse.

2.5. Databeskyttelsesordningen

a) Anvendelse af rammeafgårelsen om databeskyttelsen i tredje søjle

Da den adgang, der gives myndighederne med ansvar for den indre sikkerhed, er en undtagelse fra VIS' formål, bør den være underlagt en konsekvent databeskyttelsesordning, der sikrer et højt beskyttelsesniveau for de data, der findes i VIS og behandles af de nationale myndigheder eller af Europol.

Ifølge forslaget artikel 8 skal Rådets rammeafgårelse om beskyttelse af personoplysninger i forbindelse med det politimæssige og strafferetlige samarbejde (i det følgende benævnt »rammeafgårelsen«) finde anvendelse på behandling af personoplysninger efter denne afgørelse. Med hensyn til databeskyttelse bør det foreliggende forslag således betragtes som en lex specialis, der supplerer eller tydeliggør den generelle lov (dvs. rammeafgårelsen). F.eks. er reglerne om videreoverførsel af data strengere i dette forslag og bør tages til følge. Det samme gælder for begrundelserne for adgang til dataene.

b) Anvendelsesområde

EDPS noterer sig med tilfredshed, at rammeafgårelsens databeskyttelsesordning finder anvendelse på al behandling af personoplysninger i henhold til den foreslåede afgørelse. Det betyder, at databeskyttelsesniveauet skal være ækvivalent, uanset hvilke myndigheder der søger data i VIS.

Da der i artikel 2 anvendes et funktionelt kriterium til definition af disse myndigheder (»de myndigheder i medlemsstaterne, der har ansvaret for forebyggelse, afsløring eller efterforskning af terrorhandlinger eller andre alvorlige strafbare handlinger«), kunne denne definition omfatte efterretningstjenester samt retshåndhavende myndigheder. Efterretningstjenester, der søger i VIS, er derfor principielt underlagt de samme forpligtelser med hensyn til databeskyttelse, hvilket helt klart er et positivt træk.

Da der imidlertid kan herske nogen tvivl om denne fortolkning vedrørende rammeafgårelsens anvendelighed på efterretningstjenester, når de får adgang til VIS-data, foreslår EDPS en alternativ ordlyd som f.eks.:

»I de tilfælde, hvor rammeafgårelsen (...) ikke finder anvendelse, skal medlemsstaterne sørge for et databeskyttelsesniveau, som mindst svarer til det niveau, der sikres i henhold til rammeafgårelsen«.

c) Tilsyn

Med hensyn til affattelsen af artikel 8 bør det tydeliggøres, at stk. 1 vedrører behandling af data inden for medlemsstaternes territorium. Stk. 2 og 3 tydeliggør anvendelsesområdet (databehandling foretaget af Europol og Kommissionen), og det bør gøres helt klart, at stk. 1 vedrører noget andet.

Det er en fornuftig fremgangsmåde at fordele tilsynsbeføjelser afhængigt af de forskellige aktørers respektive aktiviteter. Der mangler imidlertid et element: behovet for en koordineret frem-

gangsmåde for tilsynet. Som det allerede blev anført i EDPS's udtalelse om VIS: »Det er i forbindelse med tilsynet med VIS også vigtigt at understrege, at de nationale tilsynsmyndigheders og Den Europæiske Tilsynsførende for Databeskyttelses tilsynsvirksomhed i et vist omfang bør samordnes. Der er således behov for en harmoniseret gennemførelse af forordningen og for at arbejde hen imod en fælles tilgang til fælles problemer.

Artikel 35 [i VIS-forslaget] bør derfor indeholde en bestemmelse om, at Den Europæiske Tilsynsførende for Databeskyttelse indkalder til møde med samtlige nationale tilsynsmyndigheder mindst én gang om året.«

Det samme gælder for denne specifikke anvendelse af VIS-systemet (idet Europols Fælles Kontrolinstans i dette tilfælde også er involveret). Tilsynet bør være fuldstændigt på linje med tilsynet med »første søjle-VIS«, da det er det samme system. Desuden er koordinationsmøder, som indkaldes af EDPS, med alle parter involveret i tilsynet, også det forbillende, som er valgt i forbindelse med tilsyn med andre større informationssystemer, som f.eks. Eurodac.

EDPS er klar over, at man i en vis udstrækning allerede opererer med koordinering i forslaget, hvor man omtaler den rolle, som skal spilles af den fremtidige gruppe vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger, som er nedsat ved artikel 31 i den foreslåede rammeafgårelse. Det bør dog gentages, at selve tilsynet ikke er omfattet af dette rådgivende organs mission.

EDPS foreslår, at der tilføjes en bestemmelse om, at det koordinationsmøde, der indkaldes af EDPS som led i tilsynet med »første søjle-VIS«, også skal have kompetence med hensyn til data, der behandles i medfør af dette forslag, og at Europols Fælles Kontrolinstans også bør være repræsenteret i den forbindelse.

2.6. Egenkontrol

Forslagets artikel 12 indeholder bestemmelser om overvågningssystemer for VIS. EDPS mener, at denne overvågning ikke kun bør vedrøre aspekterne resultater, omkostningseffektivitet og tjenesternes kvalitet, men også overensstemmelse med juridiske krav, især på databeskyttelsesområdet. Artikel 12 bør ændres tilsvarende.

For at kunne gennemføre denne egenkontrol med databehandlingens lovlighed bør Kommissionen sættes i stand til at anvende de registre, der føres i henhold til forslaget artikel 10. Det bør derfor i artikel 10 fastsættes, at disse registre ikke kun skal opbevares for at overvåge databeskyttelsen og for at garantere oplysningernes sikkerhed, men også for at gennemføre regelmæssig egenkontrol med VIS. Egenkontrolrapporterne vil være et bidrag til den tilsynsopgave, der er pålagt EDPS og de andre tilsynsførende, som i højere grad vil være i stand til at udvælge prioritetsområderne for deres tilsyn.

3. KONKLUSION

På baggrund af ovenstående fremhæver EDPS, at det er afgørende, at de myndigheder, der har ansvaret for den indre sikkerhed, samt Europol kun får adgang i hvert enkelt tilfælde og under strenge sikkerhedsgarantier. Denne målsætning opfyldes generelt tilfredsstillende i forslaget, selv om der kan foretages visse forbedringer som foreslået i denne udtalelse:

- Det bør være en betingelse for adgang til VIS ifølge artikel 5, at søgningen vil bidrage »væsentligt« til forebyggelse, afsløring eller efterforskning af en strafbar handling, og det bør på grundlag af de registre, der kræves i artikel 10, være muligt i hvert enkelt tilfælde at evaluere dette forhold.
- To søgekommandoer for adgang til VIS, jf. artikel 5, stk. 2, nemlig: »rejsens formål« og »fotografier«, bør tages op til fornyet overvejelse og stilles til rådighed som supplerende oplysninger, når der foreligger et hit.

- Det databeskyttelsesniveau, der gælder efter søgning, bør være ækvivalent, uanset hvilke myndigheder der søger data i VIS. Artikel 8 og 10 bør også gælde for de medlemsstater, hvor VIS-forordningen ikke finder anvendelse.
- Der bør sikres en koordineret fremgangsmåde for tilsyn, også for så vidt angår VIS-adgang som skitseret i dette forslag.
- Bestemmelserne om overvågningssystemer bør også sikre, at der foretages egenkontrol med opfyldelsen af databeskyttelseskravene.

Udfærdiget i Bruxelles, den 20. januar 2006

Peter HUSTINX

*Den Europæiske Tilsynsførende for Data-
beskyttelse*