EUROPEISKA DATATILLSYNSMANNEN

Yttrande från Europeiska datatillsynsmannen om förslaget till rådets beslut om möjlighet till sökningar i informationssystemet för viseringar (VIS) för medlemsstatsmyndigheter med ansvar för inre säkerhet och för Europol för att förebygga, upptäcka och utreda terroristbrott och andra grova brott (KOM(2005) 600 slutlig)

(2006/C 97/03)

EUROPEISKA DATATILLSYNSMANNEN HAR ANTAGIT DETTA YTTRANDE

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

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

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

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

med beaktande av begäran om ett yttrande i enlighet med artikel 28.2 i Europaparlamentets och rådets förordning (EG) nr 45/2001 som mottogs den 29 november 2005 från kommissionen.

HÄRIGENOM FRAMFÖRS FÖLJANDE.

1. INLEDNING

1.1 Inledande anmärkning

Förslaget till rådets beslut om möjlighet till sökningar i informationssystemet för viseringar (VIS) för medlemsstatsmyndigheter med ansvar för inre säkerhet och för Europol för att förhindra, upptäcka och utreda terroristbrott och andra grova brott (nedan kallat ”förslaget”) sändes av kommissionen till Europeiska datatillsynsmannen i ett brev av den 24 november 2005. Datatillsynsmannen tolkar detta brev som en begäran om samråd med gemenskapsinstitutioner och gemenskapsorgan i enlighet med artikel 28.2 i förordning (EG) nr 45/2001. Enligt datatillsynsmannen bör detta yttrande nämnas i ingressen till beslutet.

Datatillsynsmannen anser att det är viktigt att lämna ett yttrande om detta känsliga ämne eftersom detta förslag är en direkt följd av inrättandet av VIS, som datatillsynsmannen kommer att övervaka och som han yttrade sig om den 23 mars 2005 ([1]). Redan i det yttrandet diskuterades hypotesen att brottsbekämpande myndigheter skulle få tillgång till systemet (se nedan). Skapandet av nya åtkomsträttigheter till VIS kommer att få avgörande konsekvenser för systemet när det gäller dataskydd. Yttrandet om detta förslag är därför en nödvändig uppföljning av det första yttrandet.

1.2 Förslagets betydelse

a) *Bakgrund*

Förslaget är viktigt inte bara som ett självständigt förslag utan också för att det ligger inom den allmänna trenden att bevilja tillgång för brottsbekämpande myndigheter till flera storskaliga informations- och identifieringssystem. Detta nämns bl.a. i kommissionens meddelande av den 24 november 2005 om större effektivitet, förbättrad interoperabilitet och synergieffekter mellan EU:s databaser på området rättsliga och inrikes frågor ([2]), särskilt i punkt 4.6: ”*Med tanke på målsättningen att bekämpa terrorism och brottslighet ser rådet nu det som en brist att uppgifterna i VIS inte kan användas av de myndigheter som ansvarar för den inre säkerheten. Detta gäller även uppgifter om invandring i SIS II och uppgifter i Eurodac.*”

Förslaget kan därför ses som en föregångare till liknande rättsliga instrument som utvecklas när det gäller andra databaser, och det är ytterst viktigt att från början fastställa i vilka fall sådan tillgång skulle kunna tillåtas.

([1]) Europeiska datatillsynsmannens yttrande om Europaparlamentets och rådets förordning om informations-systemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (KOM(2004) 835 slutlig).

([2]) KOM(2005) 597 slutlig.

b) *Konsekvenser av nya åtkomsträttigheter till VIS*

Datatillsynsmannen är givetvis medveten om att de brottsbekämpande myndigheterna behöver tillgång till bästa möjliga verktyg för att identifiera personer som begår terroristhandlingar eller andra grova brott. Datatillsynsmannen är också medveten om att VIS-uppgifter under vissa omständigheter kan utgöra en viktig informationskälla för dessa myndigheter.

Hur motiverat det än må vara med tanke på kampen mot terrorismen är det emellertid inte ett obetydligt steg att ge brottsbekämpande myndigheter tillgång till databaser inom första pelaren. Man måste beakta att VIS är ett informationssystem som har utvecklats för tillämpningen av den europeiska viseringspolitiken och inte som ett instrument för brottsbekämpning. Rutinmässig tillgång skulle helt klart utgöra ett allvarligt brott mot principen om begränsning av ändamålet. Det skulle innebära en oproportionerlig kränkning av den personliga integriteten för resande som samtycker till att deras uppgifter behandlas för att de skall få en visering, och som förväntar sig att deras uppgifter samlas in, granskas och översänds endast för det ändamålet.

Eftersom informationssystem är konstruerade för ett visst ändamål, med skyddsåtgärder, säkerhet och villkor för tillgång som är fastställda med tanke på detta ändamål, skulle beviljandet av systematisk tillgång för ett annat ändamål än det ursprungliga inte endast utgöra ett brott mot principen om begränsning av ändamålet, utan det skulle också kunna innebära att dessa försiktighetsåtgärder blir olämpliga eller otillräckliga.

Enligt samma resonemang skulle en sådan betydande förändring av systemet kunna leda till att resultaten av konsekvensbedömningen (som endast gällde användningen av systemet för det ursprungliga ändamålet) blir ogiltiga. Detsamma gäller yttrandena från dataskyddsmyndigheterna. Man skulle kunna hävda att det nya förslaget ändrar förutsättningarna för den undersökning av förenligheten som dessa utfört.

c) *Strikt begränsning av tillgången*

Mot denna bakgrund vill datatillsynsmannen betona att tillgång till VIS för brottsbekämpande myndigheter endast kan beviljas under särskilda omständigheter, från fall till fall, och att strikta skyddsåtgärder måste vidtas. Med andra ord måste sökningar som görs av brottsbekämpande organ begränsas till specifika ärenden med lämpliga tekniska och rättsliga medel.

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

Sammanfattningsvis är de väsentliga kraven följande:

— Systematisk tillgång bör inte beviljas. Beslutet måste garantera att man alltid i varje enskilt fall bedömer om det är nödvändigt och rimligt att ge myndigheter inom tredje pelaren tillgång till systemet. I detta hänseende är det ytterst viktigt att rättsakten formuleras mycket noga så att det inte finns något utrymme för en bred tolkning som i sin tur leder till rutinmässig tillgång.

— I de fall då tillgång beviljas måste lämpliga skyddsåtgärder och villkor tillämpas, inklusive ett omfattande dataskyddssystem för nationell användning av uppgifterna, med tanke på att sådan tillgång är av känslig natur.

1.3 **Inledande synpunkter**

Datatillsynsmannen är medveten om att dataskydd har ägnats stor uppmärksamhet i detta förslag till rättsakt, huvudsakligen genom att tillgången begränsas till specifika ärenden och endast medges i syfte att bekämpa grov brottslighet ([1]).

Bland de andra positiva inslagen vill datatillsynsmannen också särskilt nämna

— begränsningen till vissa former av brott som anges i Europolkonventionen,

— skyldigheten för medlemsstaterna att sammanställa en förteckning över myndigheter som har tillgång till systemet och att offentliggöra dessa förteckningar,

— inrättandet av en central åtkomstpunkt i varje medlemsstat (och en specialenhet inom Europol) för att möjliggöra noggrannare prövning av framställningar om tillgång samt bättre övervakning,

— strikta regler för vidareöverföring av uppgifter enligt artikel 8.5 i förslaget,

— skyldigheten för medlemsstaterna och Europol att föra register över de personer som ansvarar för sökningarna bland uppgifterna.

2. **ANALYS AV FÖRSLAGET**

2.1 **Inledande anmärkning**

I syfte att medge tillgång för myndigheter på grundval av tredje pelaren bör huvudförslaget om VIS avseende första pelaren innehålla en övergångsklausul som i huvudsak fastställer det möjliga innehållet i en rättsakt inom tredje pelaren såsom detta förslag. När datatillsynsmannen lämnade sitt yttrande om VIS hade denna övergångsklausul ännu inte införts, och datatillsynsmannen kunde inte lämna synpunkter på den. Alla nedanstående synpunkter lämnas därför med förbehåll för innehållet i övergångsklausulen.

([1]) Detta överensstämmer också med rådets slutsatser från mars och juli 2005, där det begärdes att myndigheter med ansvar för inre säkerhet skulle beviljas tillgång till VIS *"under strikt iakttagande av bestämmelserna om skydd av personuppgifter"*.

2.2 **Ändamålet med tillgången**

För att säkerställa en lämplig begränsning av tillgången är det viktigt att noga fastställa villkoren för tillgång till VIS. Datatillsynsmannen välkomnar att det, inte enbart i själva förslaget till beslut utan även i motiveringen och skälen (särskilt skäl 7), tydligt klargörs att avsikten är att medge tillgång endast från fall till fall.

En synpunkt kan lämnas på artikel 5 i förslaget för att styra tolkningen av denna.

Artikel 5 begränsar omfattningen av tillgången genom följande villkor:

b) Sökningarna måste vara nödvändiga för att förebygga, upptäcka eller utreda terroristbrott eller andra grova brott.

c) Sökningarna måste vara nödvändiga i ett specifikt ärende. (…)

d) Det måste, på grundval av faktiska indikationer, finnas rimliga skäl att anse att en sökning av VIS-uppgifter kommer att bidra till att brotten i fråga förebyggs, upptäcks eller utreds.

Dessa villkor är kumulativa, eftersom villkoret under b snarare är en avgränsning av det materiella tillämpningsområdet. I praktiken innebär det att en myndighet som önskar få tillgång till VIS måste ha att göra med ett grovt brott enligt b i förslaget, och det måste finnas ett specifikt ärende enligt c. Dessutom måste myndigheten kunna visa att sökningar av VIS-uppgifter i detta specifika ärende kommer att bidra till att brottet i fråga förebyggs, upptäcks eller utreds i enlighet med d.

Även med denna tolkning av artikel 5 är datatillsynsmannen oroad över den flexibla lydelsen i punkt d: ”bidra till” är ett ganska brett uttryck. Det finns många fall då VIS-uppgifter skulle ”bidra till” att ett grovt brott förebyggs eller utreds. För att det skall vara motiverat att ge tillgång till VIS-uppgifter genom undantag från principen om begränsning av ändamålet anser datatillsynsmannen att sådana sökningar ”i väsentlig grad bör bidra till” att brottet i fråga förebyggs, upptäcks eller utreds, och föreslår att artikel 5 skall ändras i enlighet med detta.

I artikel 10 föreskrivs att det exakta ändamålet med sökningen skall anges i register. Det ”exakta ändamålet” bör innefatta de faktorer som gjorde det nödvändigt att göra sökningar i VIS i enlighet med artikel 5 d. Detta skulle bidra till att garantera att en nödvändighetsprövning tillämpas för alla sökningar i VIS, och minska risken för rutinmässig tillgång.

2.3 **Söknycklar för VIS-databasen**

I artikel 5.2 och 5.3 föreskrivs ett system för tillgång till VIS-uppgifter i två steg, där en uppsättning uppgifter blir tillgänglig endast om en sökning på grundval av den första uppsättningen uppgifter har gett en träff. Detta är i sig en klok strategi. Den första uppsättningen uppgifter förefaller emellertid vara mycket generell. Man kan särskilt ifrågasätta relevansen av följande uppgifter som anges i 5.2 e och i för den första uppsättningen uppgifter:

— ”Syftet med resan” förefaller vara en alltför allmän nyckel för att möjliggöra effektiva sökningar i systemet. Dessutom medför den en risk att resande profileras på grundval av denna uppgift.

— När det gäller ”fotografier” är möjligheten till sökningar på grundval av fotografier begränsad i en så stor databas. Med nuvarande teknik ger sådana sökningar ett oacceptabelt antal falska matchningar. Konsekvenserna av en felaktig identifiering är mycket allvarliga för personen i fråga.

Datatillsynsmannen begär därför att uppgifterna i artikel 5.2 e och i betraktas som kompletterande information som blir tillgänglig om den första sökningen visar att det redan finns uppgifter i systemet, och att de flyttas till artikel 5.3.

Ett annat alternativ är att tillåta sökningar i databasen på grundval av fotografier endast på villkor att den rådgivande kommittén gör en bedömning av tekniken, och först när denna teknik utvecklats och kan anses tillräckligt tillförlitlig.

2.4 **Tillämpning på medlemsstater som inte omfattas av VIS-förordningen**

Myndigheter med ansvar för inre säkerhet i medlemsstater som inte deltar i VIS kan ges tillgång till VIS för sökningar. Dessa myndigheter måste utföra sökningarna via en deltagande medlemsstat, med iakttagande av de regler som fastställs i artikel 5.1 b–d (dvs. endast från fall till fall), och måste lämna in en välmotiverad skriftlig begäran.

Datatillsynsmannen vill betona att det är nödvändigt att införa ett antal villkor för ytterligare behandling utöver sökningarna. Den regel som gäller för medlemsstater som deltar i VIS är att uppgifter som har hämtats från VIS måste behandlas i enlighet med rambeslutet om skydd av personuppgifter inom tredje pelaren (se nedan). Samma villkor bör gälla för medlemsstater som inte omfattas av VIS-förordningen, men som söker uppgifter i systemet. Samma princip bör tillämpas när det gäller registerföring för framtida övervakning. Datatillsynsmannen rekommenderar därför att man lägger till en punkt i artikel 6 i förslaget där det anges att artiklarna 8 och 10 i beslutet även skall gälla för medlemsstater som inte omfattas av VIS-förordningen.

2.5 **Dataskyddssystem**

a) *Tillämpning av rambeslutet om skydd för personuppgifter inom tredje pelaren*

Eftersom tillgången till systemet för myndigheter med ansvar för inre säkerhet utgör ett undantag från ändamålet med VIS bör denna tillgång omfattas av ett konsekvent dataskyddssystem som garanterar en hög skyddsnivå för uppgifter som hämtas från VIS och behandlas av nationella myndigheter eller Europol.

I artikel 8 i förslaget fastställs att rådets rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (nedan kallat rambeslutet) skall gälla för behandling av uppgifter enligt förslaget till beslut. När det gäller dataskydd bör detta förslag alltså betraktas som en *lex specialis*, som kompletterar eller preciserar en *lex generalis* (dvs. rambeslutet). Reglerna om vidareöverföring av uppgifter är exempelvis striktare i detta förslag och bör följas. Detsamma gäller skälen för att ge tillgång till uppgifterna.

b) *Tillämpningsområde*

Datatillsynsmannen välkomnar att dataskyddssystemet i rambeslutet gäller för all behandling av personuppgifter i enlighet med förslaget till beslut. Det betyder att dataskyddsnivån skall vara likvärdig oavsett vilka myndigheter som gör sökningar i VIS-uppgifterna.

Eftersom man i artikel 2 använder ett funktionellt kriterium för att definiera dessa myndigheter (”myndigheter i medlemsstaterna som är ansvariga för att förebygga, upptäcka eller utreda terroristbrott eller andra grova brott”) kan denna definition innefatta både underrättelsetjänster och brottsbekämpande myndigheter. Följaktligen gäller i princip samma skyldigheter i fråga om dataskydd för underrättelsetjänster som gör sökningar i VIS, vilket naturligtvis är ett positivt inslag.

Eftersom det kan finnas vissa tvivel när det gäller denna tolkning av rambeslutets tillämplighet på underrättelsetjänster när de gör sökningar i VIS, föreslår emellertid datatillsynsmannen en alternativ lydelse, exempelvis:

”Om rambeslutet (…) inte är tillämpligt skall medlemsstaterna föreskriva en dataskyddsnivå som åtminstone motsvarar den nivå som garanteras enligt rambeslutet.”

c) *Tillsyn*

När det gäller lydelsen i artikel 8 bör det klargöras att punkt 1 gäller behandling av uppgifter inom medlemsstaternas territorium. Tillämpningsområdet för punkterna 2 och 3 (databehandling inom Europol och kommissionen) klargörs i dessa punkter, och det bör uttryckligen anges att punkt 1 gäller en annan hypotes.

Det är en god idé att fördela tillsynsbefogenheterna i enlighet med de olika aktörernas verksamhetsområden. Ett inslag saknas emellertid, nämligen behovet av en samordnad strategi för övervakning, vilket redan har påpekats i datatillsynsmannens yttrande om VIS: ”*När det gäller tillsynen av VIS är det även viktigt att framhålla att de nationella tillsynsmyndigheternas och datatillsynsmannens tillsyn bör samordnas i viss mån. Det är nödvändigt med ett harmoniserat genomförande av förordningen och att man verkar för ett gemensamt tillvägagångssätt när det gäller gemensamma problem.*

Artikel 35 [i VIS-förslaget] bör innehålla en bestämmelse om detta där det fastställs att datatillsynsmannen skall sammankalla ett möte med alla nationella tillsynsmyndigheter, minst en gång varje år.”

Detta gäller även denna särskilda användning av VIS-systemet (i detta fall även med deltagande av Europols gemensamma tillsynsmyndighet). Tillsynen bör helt överensstämma med övervakningen av ”VIS inom första pelaren”, eftersom det är samma system. Vidare är samordningsmöten med alla parter som deltar i övervakningen, med datatillsynsmannen som sammankallande, också den modell som har valts för övervakningen av andra storskaliga informationssystem, exempelvis Eurodac.

Datatillsynsmannen är medveten om att en viss samordning planeras i förslaget, där man nämner de uppgifter som skall utföras av den framtida arbetsgruppen för skydd av enskilda med avseende på behandling av personuppgifter, vilken inrättas genom artikel 31 i förslaget till rambeslut. Det bör emellertid upprepas att själva övervakningen inte ingår i detta rådgivande organs uppdrag.

Datatillsynsmannen föreslår att man lägger till en bestämmelse där det fastställs att det samordningsmöte som datatillsynsmannen sammankallar inom ramen för övervakningen av ”VIS inom första pelaren” också skall vara behörigt när det gäller uppgifter som behandlas enligt detta förslag, och att Europols gemensamma tillsynsmyndighet därför bör vara företrädd.

2.6 **Egenkontroll**

I artikel 12 i förslaget föreskrivs övervakningssystem för VIS. Datatillsynsmannen anser att denna övervakning inte enbart bör gälla produktivitet, kostnadseffektivitet och tjänsternas kvalitet, utan även efterlevnaden av rättsliga krav, särskilt när det gäller dataskydd. Artikel 12 bör ändras i enlighet med detta.

För att utföra denna egenkontroll av behandlingens laglighet bör kommissionen få möjlighet att använda de register som förs i enlighet med artikel 10 i förslaget. I artikel 10 bör det därför föreskrivas att dessa register skall föras inte endast för tillsyn av dataskyddet och för att garantera datasäkerhet utan även för regelbunden egenkontroll av VIS. Rapporterna över egenkontrollen kommer att underlätta datatillsynsmannens och de andra tillsynsmyndigheternas arbete eftersom de får bättre möjlighet att välja prioriterade områden för tillsynen.

3. **SLUTSATS**

Mot denna bakgrund betonar datatillsynsmannen att det är ytterst viktigt att myndigheter med ansvar för inre säkerhet samt Europol endast beviljas tillgång till systemet från fall till fall och med tillämpning av strikta skyddsåtgärder. Detta mål uppnås på det hela taget med förslaget, även om vissa förbättringar kan införas, enligt följande förslag i detta yttrande:

— Ett villkor för tillgång till VIS enligt artikel 5 bör vara att sökningarna i ”väsentlig grad” bidrar till att ett grovt brott förebyggs, upptäcks eller utreds, och de register som föreskrivs i artikel 10 bör möjliggöra en bedömning av detta villkor i varje enskilt fall.

— Två söknycklar för tillgång till VIS som nämns i artikel 5.2, nämligen ”syftet med resan” och ”fotografier” bör övervägas på nytt och göras tillgängliga som kompletterande information om en sökning ger en träff.

— En likvärdig dataskyddsnivå bör gälla för behandling utöver sökningar oavsett vilka myndigheter som söker uppgifter i VIS. Artiklarna 8 och 10 bör även gälla medlemsstater som inte omfattas av VIS-förordningen.

— En samordnad strategi för övervakning bör garanteras, även när det gäller tillgång till VIS i enlighet med detta förslag.

— Bestämmelser om övervakning bör också säkerställa egenkontroll av efterlevnaden av dataskyddskraven.

Bryssel den 20 januari 2006

Peter HUSTINX

Europeisk datatillsynsman