

(Ekstern oversættelse)

EUROPA-PARLAMENTET

2004



2009

Udvalget om Borgernes Rettigheder og Retlige og Indre Anliggender

15.3.2005

ARBEJDSDOKUMENT

om forslag til Europa-Parlamentets og Rådets forordning om visuminformationssystemet (VIS) og udveksling af oplysninger mellem medlemsstaterne om visa til kortvarigt ophold: databeskyttelse, forvaltningsmæssige problemer samt problemer i et bredere perspektiv

Udvalget om Borgernes Rettigheder og Retlige og Indre Anliggender

Ordfører: Sarah Ludford

II. Databeskyttelse og forvaltningsmæssige problemer

Der er muligheder, men også risici ved brugen af biometriske data. Ud over de sædvanlige bekymringer over datafortrolighed er brugen af biometriske data en indtrængning i den private sfære, og den forstyrrer borgernes anonymitet på en særligt akut måde. Det er nødvendigt med et effektivt kontrolsystem mod lækage, ikke-autoriseret adgang og generel overvågning, og det er nødvendigt med klare aftaler med henblik på rettelser. Der kan være overdrevne forventninger til, hvad man kan opnå med biometri samt en falsk følelse af sikkerhed omkring troværdigheden. Men eksperter peger også på, at brugen af biometriske data har potentiale til en bedre sikring af privatlivets fred, eftersom de kan tillade autentifikation uden nødvendigvis at afsløre en persons identitet.

II.1 Biometriske data i VIS

Kommissionen foreslog, at alfanumeriske oplysninger (navn, fødselsdato osv.) skulle være klar til implementering i december 2006, og at to biometriske identifikatorer (fingeraftryk og ansigtsscanninger) skulle være klar til implementering i december 2007. Men på grund af problemet med 'sammenstød' af biometriske visa har RIA-Rådet besluttet at fremskynde indkøringen af biometriske data i visuminformationssystemet til 2006.¹

Der anmodes om stillingtagen til brug og potentielt misbrug af biometriske data i VIS, om hvorvidt det er nødvendigt med to identifikatorer, hvilken type og mængde, dvs. om der skal være to eller 10 fingeraftryk.² Ordføreren ønsker at trække på flere forestående rapporter om biometriske data fra Kommissionens Fælles Forskningscenter, udnævnt af LIBE-udvalget, samt en rapport om VIS og biometriske data fra Artikel 29-Gruppen og endelig en rapport fra EU's Tilsynsførende for Databeskyttelse.

II.2 Datalagring (artikel 20)

Rådets konklusioner fra februar 2004 fastsætter målet for lagring af data til mindst fem år, men Kommissionens forslag gør femårsreglen til den fremherskende. Det forklarer nødvendigheden af en femårig datalagringsperiode med den begrundelse, at visa til kortvarigt ophold i særlige tilfælde kan være gyldige i op til fem år³. Men Kommissionen forudser også en datalagringsperiode på mindst fem år, hvis der er givet afslag på visum.⁴

I sin udtalelse fra august 2004 om VIS argumenterede Artikel 29-Gruppen dog for proportionalitetsprincippet og anførte, at fem års datalagring burde være et maksimum og ikke et minimum. Arbejdsgruppen foreslog, at lagringskriterierne for forskellige situationer, der kunne opstå i det virkelige liv, skulle være mere sofistikerede, hvis det kunne forenkle ansøgningsproceduren, f.eks. et specifikt kriterium for personer, der rejser

¹ RIA-Rådets møde af 24.2.2005.

² Undersøgelse til fastlæggelse af den mere omfattende virkning af visuminformationssystemet, EPEC's endelige rapport, december 2004, s. 76.

³ Fælles konsulære instrukser (CCI), del V, punkt 2.1; i: EUT C 310 af 19.12.2003, s. 1.

⁴ CCI, del VII, punkt 2.

(Ekstern oversættelse)

ofte.¹ Der anmodes om stillingtagen til, hvorvidt den foreslåede datalagringsperiode er passende. Vil det være bedre med en differentieret frem for en overordnet holdning til datalagringsperioder? I sit udkast til rapporten vil ordføreren indrage Artikel 29-Gruppens anden holdning til fremlæggelse i midten af april.

II.3 Forvaltning og placering af VIS (artikel 23)

Kommissionens forslag er uklart i forhold til, hvem der skal stå for den strategiske forvaltning af store it-systemer som f.eks. VIS. Spørgsmålet er blevet debatteret i en rum tid nu, og tre mulige løsninger har været drøftet under debatten om udviklingen af Schengen-informationssystem II (SIS II)², herunder:

- A) Forvaltning under Rådet
- B) Forvaltning under Kommissionen (f.eks. under enheden for store informationssystemer i GD Retlige anliggender, Frihed og Sikkerhed)
- C) et uafhængigt organ
og endelig den mulighed, der blev fremlagt i Kommissionens forslag til de finansielle overslag 2007–2013³, om
- D) forvaltning via Agenturet for Forvaltning af det Operative Samarbejde ved de Ydre Grænser.

Udviklingen af SIS II er også forbundet med dette tema i lyset af Rådets målsætning om, at de to skulle udvikles på en fælles teknisk platform, hvilket betyder, at de skal placeres samme sted. Hvad angår SIS II, mener Rådet, at det skal forblive i Strasbourg.⁴ Der anmodes om stillingtagen til, hvem der skal forvalte den centrale enhed, og hvor den skal placeres.

III: Bredere problemstillinger

III.1 *Function Creep*

Function creep er anden anvendelse af data end oprindeligt tænkt. Som skitseret ovenfor kan data lagret til ét formål senere anvendes til andre formål. I dette tilfælde kan de bidrage til kampen mod kriminalitet og terrorisme.⁵ Denne trinvis metode kan resultere i, at VIS udvikler sig til et 'overordnet efterretningsværktøj'. Er dette ønskeligt? Hvilke konsekvenser kan det få for tilliden mellem borger og stat?

Man kan allerede nu konstatere *function creep* i eksisterende EU-databaser. I et dokument fra formandskabet til SIS-gruppen står der:

Da SIS blev etableret, var det med det ene formål at fungere som

¹ Artikel 29-Gruppens holdning 7/2004, august 2004.

² KOM(2003)0771.

³ KOM (2004)0487, s. 20.

⁴ RIA-Rådets møde af 29.4.2004.

⁵ Rådsdokument 6075/05, s. 1.

(Ekstern oversættelse)

kompensationsforanstaltning ved åbning af grænserne. Lige siden, og ikke mindst fordi SIS har vist sig at være et nyttigt og effektivt værktøj, er der sket en voksende erkendelse af muligheden for en maksimering af SIS' potentiale, hovedsagelig inden for rammerne af politisamarbejdet.

De tydeligste eksempler på dette er de krav, der går ud på at udvide adgangen til SIS-data til andre myndigheder end de oprindeligt tiltænkte. Det drejer sig primært om myndigheder, [...] der kan drage nytte af oplysninger [om] en person, [der] figurerer i SIS og endvidere forbedre effektiviteten. Det er klart, at en sådan adgang skal overvejes grundigt, ikke kun af åbenlyse databeskyttelsesårsager, men også for at undgå, at en alt for bred adgang til SIS kan resultere i mindre værdifulde SIS-data og et mindre effektivt informationssystem. Ikke desto mindre er man nu i vid udstrækning enig om at benytte SIS-data til andre formål end de oprindeligt tænkte og særligt til opklarende politiarbejde i et bredt perspektiv, hvilket ydermere følger af Rådets konklusioner efter begivenhederne den 11. september 2001.¹

I et andet eksempel står der i et notat fra den tyske delegation ved Eurodac:

(e) Fremtidig anvendelse af data lagret i den centrale Eurodac-database til politi-formål

Integrationen af data lagret i Eurodac-databasen vil muliggøre en sammenligning mellem politiets fund og fingeraftryk fra personer, der søger asyl i andre medlemsstater. Dette vil i høj grad gøre det nemmere at retsforfølge og gøre det muligt at eliminere sikkerhedsrisici på et tidligt tidspunkt. Enhver anvendelse af disse data i strafferetligt øjemed har indtil videre været udelukket, eftersom Eurodac-forordningen udelukkende er kædet sammen med Dublin-konventionen. Indtil nu er disse data kun blevet brugt til at afgøre, hvilke medlemsstater der er ansvarlige for at gennemgå ansøgninger under asylproceduren. Kommissionen skal fremsætte specifikke ændringsforslag snarest muligt.²

Hvis der på nuværende tidspunkt fastlægges metoder, der omfatter adgang til data for de myndigheder, der ikke p.t. har adgang, bliver det svært senere at nægte dette, eftersom der altid vil være praktiske begrundelser for adgang. Skal vi derfor med vilje vælge en teknologi eller retlige sikkerhedsforanstaltninger i dag for at forhindre *function creep* i morgen? I denne sammenhæng er det vigtigt at bemærke, at Eurodacs standard for fingeraftryk er den samme som den, der benyttes af Interpol og nationale politimyndigheder.³

III.2 Fælles teknisk platform og interoperabilitet

En lignende betragtning fremkalder bekymring over fælles tekniske platforme,

¹ Rådsk dokument 5968/02, s. 2.1.

² Rådsk dokument 8784/02, s. 3 (e).

³ Eurodac - Rådets forordning (EF) nr. 407/2002 af 28. februar 2002, EFT L 062 , 05/03/2002, s. 1-5 Interpol - <http://www.interpol.int/Public/Forensic/fingerprints/RefDoc/default.asp>
<http://www.interpol.int/Public/ICPO/GeneralAssembly/Agn66/Resolutions/AGN66RES8.asp>.

interoperabilitet og konsekvensen af 'princippet om tilgængelighed' for it-systemer.¹

Der er planlagt en fælles teknisk platform mellem Schengen-informationssystem II (SIS II) og VIS. Europa-Kommissionen besluttede at sammenlægge SIS II- og VIS-kontrakten, hvad angår teknisk design, udvikling og anvendelse, og gav kontrakten til et konsortium under franske Steria og belgiske Hewlett Packard med et budget på 40 millioner euro. Systemet er allerede under opbygning, men hvordan er det overhovedet muligt, når der ikke er nogen præcis definition af, hvad det i sidste ende skal indeholde? Efter al sandsynlighed vil det være beregnet til at indeholde den maksimale datamængde, således at den kapacitet, der ikke bliver anvendt i begyndelsen, vil være til rådighed til senere brug.

Dette er rent faktisk, hvad rådsdokumenter tilkendegiver. Haag-programmet påpeger, at metoder til udveksling af oplysninger skal udnytte den nye teknologi fuldt ud og være tilpasset alle informationstyper, alt efter behov, via gensidig adgang til eller interoperabilitet i nationale databaser eller direkte (online) adgang, herunder også for Europol, til centrale EU-databaser som f.eks. SIS.² Siden Rådets konklusioner af februar 2004 har idéen om gensidig adgang til it-systemer været på dagsordenen. SIS II/VIS-tilslutningsundersøgelser samt den kommende kommissionsmeddelelse vedrørende interoperabilitet peger alle i retning af, at alle databaser med tiden bliver sammenkørt (SIS, VIS, Europol, pas, PNR-data, kørekort, personnummerbeviser), og at eksisterende data vil blive anvendt til nye formål.

IV. Oversigt over det samlede planlagte system

På denne baggrund tillader ordføreren sig at påstå, at Europa-Parlamentet har behov for at se hele billedet, før det tager en beslutning om VIS-forslaget isoleret set. En effektiv drift afhænger af et komplekst sæt foranstaltninger, som Kommissionens forslag forventes at indeholde:

- (i) nævnt i Kommissionens forslag som nødvendige tillæg til VIS:
 - ændring af fælles konsulære instrukser til standarder og procedurer for indhentning af biometriske data, herunder registreringen af biometriske data
 - udvikling af en supplerende mekanisme til udveksling af data med Irland og UK (som ikke er med i VIS-ordningen)
 - Kommissionens forslag om udveksling af data for visa til langvarigt ophold
- (ii) Kommissionsmeddelelse om interoperabilitet i december 2005.
- (iii) Rådet har bedt Kommissionen fremlægge
 - et søjle 3-forslag vedrørende beskyttelse af personlige data og
 - et søjle 3-forslag vedrørende adgang for politimyndigheder.³

¹ Haag-programmet fastslår, at i henhold til 'princippet om tilgængelighed' kan data fra en medlemsstat fra 1. januar 2008 deles med politimyndigheder i andre medlemsstater.

² Haag-programmet, afsnit 2.1.

³ Rådsdokument 6810/05.

(Ekstern oversættelse)

Det er ganske sikkert afgørende for Europa-Parlamentet, der har fælles beslutningsprocedure for dette forslag, at det har fuld forståelse for, hvad disse seks øvrige foranstaltninger (og andre mulige) betyder for driften af VIS, især interoperabiliteten.¹ Ordføreren husker, at en tidligere ordfører meddelte, at han ikke var i stand til at godkende forslaget om biometriske data i visa, da han ikke mente, at de grundlæggende krav til oplyst beslutningstagning var opfyldt på grund af mangel på nødvendige oplysninger (i sager om falske visa, omkostninger og fejlprocenter) med henblik på vurdering af, om målene kunne nås på en mere rimelig og mindre påtrængende måde.²

Der er ingen anvendelse af biometriske teknologier, selv ikke dem, der vurderes til at være store, som f.eks. FBI's fingeraftryksdatabase i USA, der blot tilnærmelsesvis kommer op i den størrelsesorden, der er foreslået eller planlagt for EU-pas og visa. Det er vigtigt at gøre det rigtigt.

¹ http://europa.eu.int/comm/off/work_programme/catalogue_2005_01_27.pdf, s. 70.

² Udkast til betænkning af Ole Sørensen af 10.3.2004 om Kommissionens forslag om vedtagelse af Rådets forordning om ændring af forordning (EF) 1030/2002 om ensartet udformning af opholdstilladelser til tredjelandsstatsborgere (KOM(2003)0558 – C5-0467/2003 – 2003/0218(CNS)) samt Kommissionens forslag om vedtagelse af Rådets forordning om ændring af forordning (EF) 1683/95 om ensartet udformning af visa (KOM(2003)0558 – C5-0466/2003 – 2003/0217(CNS)) (PE 329.955).