INSTITUT FOR
MENNESKERETTIGHEDER

STRANDGADE 56 · 1401 KØBENHAVN K
TLF. 32 69 88 88
FAX 32 69 88 00
CENTER@HUMANRIGHTS.DK
WWW.MENNESKERET.DK
WWW.HUMANRIGHTS.DK

Integrationsministeriet,
Lovkontoret
Holbergsgade 6
1057 - Kbh. K

DATO 3. marts 2008
J.NR
540.60/17393

Vedr.: Udkast til forslag til ændring af udlændingeloven

Ved skrivelse af 22. februar 2008 fremsendte Integrationsministeriet Udkast til forslag til ændring af udlændingeloven (Gennemførelse af VIS-forordningen m.m.) af 21. februar 2008 til Institut for Menneskerettigheder med anmodning om Instituttets eventuelle kommentarer hertil.

Med udkastet til ændringsloven gennemføres en forhåndsinkorporering af to endnu ikke vedtagne forordninger, der begge anføres at være en udbygning af Schengen-regelsættet, hvorfor en dansk tiltræden kan ske ved anvendelse af den særlige *opt in*-beføjelse, jf. de foreslåede nye bestemmelser i Udlændingelovens § 2 a, stk. 4 og 5, samt af en – ligeledes ikke vedtaget – rådsafgørelse, jf. den foreslåede bestemmelse i lovens § 2 a, stk. 6, med et dertil knyttet samtykke meddelt i henhold til Grundlovens § 19. Samtlige tre retsakter omhandler etablering, drift og anvendelse af Visuminformationssystemet (VIS). Hertil kommer en bemyndigelsesbestemmelse, jf. § 2 a, stk. 7, samt en regel om private virksomheders varetagelse af opgaver med modtagelse og registrering af af visumansøgninger m.v. på vegne af en dansk repræsentation, jf. § 47, stk. 3.

Institut for Menneskerettigheder finder, at udkastet ikke giver anledning til kommentarer af menneskesretlig karakter.

Der henvises til ministeriets j.nr. 2003/4050-435.

Med venlig hilsen

Kim U. Kjær

DATATILSYNET

Integrationsministeriet
(inm@inm.dk)
Dorte Larsen
(dla@inm.dk)

3. november 2003

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-post
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2003-849-0044
Sagsbehandler
Christian Wiese
Svanberg
Direkte 3319 3233

Vedrørende udarbejdelsen af VIS-systemet

Ved VIS-arbejdsgruppens møde afholdt den 21. oktober 2003 i Integrationsministeriet anmodede Integrationsministeriet om at modtage de deltagende myndigheders bemærkninger til de foreliggende oplysninger vedrørende oprettelsen af VIS-systemet med henblik på udarbejdelsen af et varslingsnotat til Regeringens Økonomiudvalg.

Som aftalt med Integrationsministeriet i forlængelse af mødet den 21. oktober 2003 skal Datatilsynet anmode om, at tilsynets udtalelse vedlægges varslingsnotatet som bilag.

Datatilsynet skal udtale følgende:

1. Persondataloven

Persondataloven[1] gælder ifølge lovens § 1, stk. 1, for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling, og for ikke-elektronisk databehandling af personoplysninger, der er eller vil blive indeholdt i et register.

Persondataloven implementerer EF-direktivet om behandling af personoplysninger i dansk ret. Databeskyttelsesdirektivet[2] pålægger medlemsstaterne en forpligtelse til at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder, især retten til privatlivets fred, i forbindelse med behandling af personoplysninger. På en række punkter indeholder databeskyttelsesdirektivet bestemmelser, som medlemsstaterne ikke kan fravige.

For så vidt angår den nationale del af det foreslåede VIS-system antager Datatilsynet i det følgende, at Udlændingestyrelsen vil være dataansvarlig myndighed for de behandlinger af personoplysninger, der foretages i forbindelse med behandlingen af visumansøgninger i VIS-systemet. Udenrigsministeriet og dets repræsentationer samt Rigspolitichefen anses således i persondatalovens forstand som databehandlere, der udelukkende behandler personoplysninger

[1] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger.
[2] Europaparlamentet 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.

vedrørende visumansøgere på vegne af den dataansvarlige, jf. persondatalovens § 3, nr. 5. Denne antagelse er baseret på den nuværende udformning af det Fælles Visumsystem (FVS), som dette foreligger anmeldt til Datatilsynet.

2. Behandling af personoplysninger i VIS-systemet

Persondatalovens § 5, som bygger på artikel 6 i databeskyttelsesdirektivet, indeholder en række grundlæggende principper for den dataansvarliges behandling af oplysninger.

Persondatalovens § 5, stk. 2, indeholder bl.a. et krav om, at indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål. Lovens § 5, stk. 3, indeholder et krav om, at oplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles.

Det er Datatilsynet opfattelse, at man ved fastlæggelsen af, hvilke oplysninger der skal behandles i VIS-systemet, nøje bør overveje, hvilke oplysninger der er relevante. Behandlingen af personoplysninger i VIS-systemet bør således udelukkende omfatte oplysninger, der sædvanligvis må antages at have relevans for behandlingen af visumansøgninger for dermed at undgå unødig dataophobning. Dette udelukker dog ikke, at andre oplysninger end dem, der sædvanligvis er relevante, i konkrete tilfælde kan anvendes i systemet, dog bør sådanne behandlinger altid ske på baggrund af en konkret vurdering.

Datatilsynet skal på denne baggrund opfordre de involverede myndigheder til så tidligt så muligt i forløbet at gøre sig de fornødne overvejelser om, hvilke oplysningstyper der som udgangspunkt bør indgå i systemet.

3. Brug af privatlivsfremmende teknologier

Datatilsynet skal i øvrigt henlede opmærksomheden på, at "Explanatory memorandum" til Kommissionens forslag om ændring af forordning 1683/95 om det ensartede visumformat og forordning 1030/02 om et ensartet format for opholdstilladelser til tredjelandsstatsborgere indeholder et afsnit om anvendelse af såkaldte privatslivsfremmende teknologier.

Datatilsynet har hidtil ikke fundet, at persondataloven medfører et generelt krav om brug af privatlivsfremmende teknologier, der sigter efter at give den registrerede mulighed for at optræde anonymt eller under et pseudonym. Datatilsynet kan dog ikke udelukke, at brug af de af Kommissionen omtalte privatlivsfremmende teknologier i visse tilfælde vil være med til at bringe en behandling i overensstemmelse med persondataloven.

Hvis forordningen kommer til at medføre krav om anvendelse af nye privatlivsfremmende teknologier, som ikke kræves i dag, vil dette formentlig også kræve flere ressourcer til etableringen af systemet.

4. Anmeldelsespligt
Det følger af persondatalovens § 43, stk. 1, at behandling af fortrolige personoplysninger, der foretages for den offentlige forvaltning, skal anmeldes til Datatilsynet forinden iværksættelsen af behandlingen. Visse behandlinger af personoplysninger er imidlertid undtaget fra anmeldelsespligten jf. § 44, stk. 1, og den i henhold til § 44, stk. 4, udstedte undtagelsesbekendtgørelse[3].

Datatilsynet har noteret sig, at VIS-systemet i sin foreliggende udformning vil skulle indeholde en række personoplysninger vedrørende visumansøgere, herunder blandt andet oplysninger i form af den registreredes billede og fingeraftryk. Derudover må det antages, at en række forskellige oplysninger kan tænkes behandlet i VIS-systemet i forbindelse med behandlingen af indgivne visumansøgninger.

Datatilsynet finder herefter umiddelbart at kunne lægge til grund, at VIS-systemet vil indeholde fortrolige og eventuelt følsomme personoplysninger.

Udlændingestyrelsen vil som dataansvarlig for de i databasen indeholdte oplysninger være forpligtet til at sikre, at behandling af personoplysninger, der finder sted i forbindelse med driften af databasen, enten er omfattet af eksisterende anmeldelser til tilsynet eller anmeldes til Datatilsynet.

5. Sikkerhed
Datatilsynet skal henlede opmærksomheden på persondatalovens kapitel 11 og de deri indeholdte bestemmelser vedrørende behandlingssikkerhed.

Det følger af persondatalovens § 41, stk. 3, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Pligten til at træffe fornødne sikkerhedsforanstaltninger påhviler efter persondatalovens § 41, stk. 3, såvel den dataansvarlige som en eventuel databehandler.

Nærmere regler om de efter persondataloven krævede sikkerhedsforanstaltninger findes i sikkerhedsbekendtgørelsen[4]. Sikkerhedsbekendtgørelsen indeholder således en række krav, som man i forbindelse med det videre arbejde med VIS-systemets udformning bør have for øje, og der bør sikres tilstrækkelige ressourcer hertil.

I den forbindelse skal det bemærkes, at i det omfang databasen er omfattet af anmeldelsespligtigen efter persondataloven, vil såvel de generelle krav i sik-

[3] Justitsministeriets bekendtgørelse nr. 529 af 15. juni 2000 om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for den offentlige forvaltning.
[4] Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

kerhedsbekendtgørelsens kapitel 1 og 2 som de skærpede krav i sikkerhedsbekendtgørelsen kapitel 3 skulle iagttages.

Særlig opmærksomhed skal i den forbindelse henledes på sikkerhedsbekendtgørelsens § 19, stk. 1, hvorefter der skal foretages maskinel registrering (logning) af alle anvendelse af personoplysninger. Registreringen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium.

Opmærksomheden henledes desuden særligt på sikkerhedsbekendtgørelsens § 14 vedrørende etableringen af eksterne kommunikationsforbindelser og de deri beskrevne krav til sikkerheden. Det følger således af sikkerhedsvejledningen[5], at der ved transmission af fortrolige oplysninger som minimum skal foretages kryptering. Hvis de transmitterede oplysninger er af følsom karakter, skal der anvendes stærk kryptering, baseret på en anerkendt algoritme.

6. Den registreredes rettigheder

Opmærksomheden skal desuden henledes på de rettigheder for den registrerede, der følger af persondataloven.

I forbindelse med driften af VIS-systemet vil den dataansvarlige eller dennes repræsentant ved indsamling af oplysninger hos den registrerede i medfør af persondatalovens § 28, stk. 1, skulle give den registrerede oplysninger om en række nærmere angivne forhold herunder særligt den dataansvarliges identitet, formålene med den behandling, hvortil oplysninger er bestemt samt alle yderligere oplysninger der under hensyn til de særlige omstændigheder, hvorunder oplysningerne er indsamlet, er nødvendige for at den registrerede kan varetage sine interesser.

Tilsvarende påhviler det i følge lovens § 29, når oplysninger ikke er indsamlet hos den registrerede, den dataansvarlige eller dennes repræsentant ved registreringen, eller hvor de indsamlede oplysninger er bestemt til videregivelse til tredjemand, senest når videregivelsen finder sted, at give den registrerede meddelelse om de ovenfor angivne forhold.

Datatilsynet forudsætter, at enhver indsamling af personoplysninger vedrørende visumansøgere i forbindelse med driften af VIS-systemet sker under iagttagelse af persondatalovens §§ 28 og 29. Opmærksomheden skal dog for god ordens skyld henledes på de i persondatalovens § 28, stk. 2, § 29, stk. 2 og 3 samt § 30, stk. 1 og 2, indeholdte undtagelser til oplysningspligten.

Efterlevelse af oplysningspligten vil efter Datatilsynets opfattelse indebære, at den registrerede skal have meddelelse på et for ham forståeligt sprog.

---

[5] Datatilsynets vejledning nr. 37 af 2. april 2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerheds om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning

Datatilsynet skal desuden henlede opmærksomheden på indsigtsretten. I medfør af persondatalovens § 31, stk. 1, skal den dataansvarlige efter begæring fra en person give meddelelse om, hvorvidt der behandles oplysninger om vedkommende. Behandles sådanne oplysninger, skal der på en let forståelig måde gives meddelelse om, hvilke oplysninger der behandles, behandlingens formål, kategorierne af modtagere af oplysningerne og tilgængelig information om, hvorfra disse oplysninger stammer. Der henvises ligeledes til de i persondatalovens § 32 indeholdte undtagelser til indsigtsretten.

Datatilsynet forudsætter, at man i forbindelse med oprettelsen af VIS-systemet vil indrette systemet på en sådan måde, at personers anmodning om indsigt i henhold til persondatalovens § 31 vil kunne blive imødekommet.

Meddelelse om indsigt skal efter persondatalovens § 32, stk. 1, som udgangspunkt gives skriftligt, hvis den registrerede anmoder herom. Som anført i rettighedsvejledningens[6] afsnit 3.4. medfører kravet om skriftlighed, at oplysningerne skal fremtræde i en sådan form, at de kan læses umiddelbart og uden brug af tekniske hjælpemidler. Heraf følger, at skriftlige meddelelser normalt bør foreligge i form af en maskinel udskrift. Meddelelsen må ikke indeholde koder m.v., som ikke er umiddelbart forståelige.

Persondataloven indeholder udover den dataansvarliges oplysningspligt og retten til indsigt en række rettigheder for den registrerede, herunder den registreredes ret til at kræve ukorrekte oplysninger rettet eller slettet, og retten til at gøre indsigelse mod, at oplysninger om vedkommende gøres til genstand for behandling. Det er den dataansvarliges pligt at sikre, at disse rettigheder ikke krænkes i forbindelse med en behandling af personoplysninger foretaget af den dataansvarlige. Der henvises i den forbindelse til rettighedsvejledningen udstedt i medfør af persondataloven.

7. Ressourcer

Det fremgår ikke på nuværende tidspunkt, hvor retsgrundlaget for VIS-systemet endnu ikke er vedtaget, om der vil blive etableret en selvstændig myndighed på EU-niveau, som skal føre tilsyn med VIS-systemet.

Hertil kommer, at indførelsen af VIS-systemet må antages at medføre et øget behov for, at Datatilsynet foretager inspektioner på danske ambassader og repræsentationer i udlandet.

Datatilsynet skal på denne baggrund bemærke, at som tilsynets bevillings- og personalemæssige situation er i dag, vil det ikke være muligt at påtage sig yderligere opgaver uden at få tilført ressourcer til dækning heraf.

---

[6] Datatilsynets vejledning nr. 126 af 19. juli 2000 om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger.

Det er Datatilsynets umiddelbare vurdering, at varetagelsen af funktionen som national tilsynsmyndighed vil belaste tilsynet på både løn- og driftsiden, og at et meget foreløbigt skøn er i størrelsesordenen 0,5 mio. kr. årligt.

Afslutningsvis skal det bemærkes, at Datatilsynets vurdering er foretaget på baggrund af det foreliggende materiale vedrørende VIS-systemet. Datatilsynet forbeholder sig således under hensyntagen til det foreliggende materiales foreløbige karakter sin endelige stillingtagen.

Datatilsynet skal anmode om at modtage arbejdsgruppens indstillinger om VIS-systemets nærmere udformning i høring, forinden disse forelægges Regeringens Økonomiudvalg.

Tilsynet skal i øvrigt anmode om at blive holdt orienteret om det videre arbejde.

Med venlig hilsen

Janni Christoffersen
Direktør

DATATILSYNET

Ministeriet for Flygtninge, Indvandrer og Integration
Holbergsgade 6
1057 København K

Sendt til: Dorte Larsen dla@inm.dk

31. januar 2005

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-post
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2005-849-0073
Sagsbehandler
Camilla Sonne Kristensen
Direkte 3319 3217

Vedrørende høring over Kommissionens forslag til forordning om et fælles europæisk visuminformationssystem (VIS) - j.nr. 2003/4050-306

Ved e-post af 14. januar 2005 har Ministeriet for Flygtninge, Indvandrere og Integration anmodet om Datatilsynets bemærkninger til forslag til forordning om et fælles europæisk visuminformationssystem (VIS) med henblik på fastlæggelse af en dansk holdning og udarbejdelse af et grundnotat til Folketingets Europaudvalg.

Datatilsynet har tidligere afgivet en udtalelse om udarbejdelsen af VIS-systemet. Der henvises til brev af 3. november 2003 til Integrationsministeriet.

Datatilsynet skal herefter udtale følgende:

1. I præambiens punkt 14 fastslås, at direktiv 95/46/EF[1] finder anvendelse på medlemsstaternes behandling af personoplysninger i medfør af forordningen, og forordningsforslaget indeholder en række konkrete bestemmelser af databeskyttelsesretlig karakter. Forslaget indeholder endvidere en grundig undersøgelse og vurdering af de proportionalitetsspørgsmål, som etablering af et så omfattende informationssystem giver anledning til.

Datatilsynet har tillige noteret sig, at de forslag, som artikel 29-gruppen er fremkommet med, er indarbejdet i forordningsforslaget.[2]

Samlet set finder Datatilsynet således, at forslaget er gennemarbejdet og tager højde for mange relevante spørgsmål af databeskyttelsesmæssig karakter.

Efter Datatilsynets opfattelse må spørgsmålet om etablering af informationssystemet, som vil omfatte store mængder personoplysninger, herunder oplys-

[1] 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

[2] Arbejdsgruppen vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger som nedsat i henhold til databeskyttelsesdirektivets artikel 29 - Opinion No. 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS)

ninger af følsom karakter, herefter i væsentlig grad bero på en vurdering af, om vægtige samfundsmæssige hensyn taler herfor. Denne vurdering finder tilsynet ikke at burde udtale sig nærmere om.

Datatilsynet har imidlertid en række bemærkninger af mere konkret karakter til forslaget, jf. nedenfor punkt 2-5.

2. Det fremgår af forslagets artikel 34, at hver medlemsstat kræver, at den eller de nationale tilsynsmyndigheder, som er oprettet i henhold til artikel 28, stk. 1, i direktiv 95/46/EF, i fuld uafhængighed og i overensstemmelse med den pågældende medlemsstats nationale ret overvåger, at den pågældende medlemsstats behandling af personoplysninger i overensstemmelse med denne forordning, herunder fremsendelsen af oplysninger til og fra VIS, foregår på lovlig vis.

Datatilsynet forudsætter umiddelbart, at der heri ligger, at persondataloven og bekendtgørelser udstedt i medfør heraf gælder *fuldt ud* for danske myndigheders behandling af personoplysninger i forbindelse med VIS.

Med hensyn til artikel 26 skal Datatilsynet endvidere gøre opmærksom på, at det af bemærkningerne fremgår, at artikel 26 i henhold til artikel 17 i direktiv 95/46/EF fastsætter, hvilke sikkerhedsforanstaltninger der skal tilvejebringes ved behandling af data.

Datatilsynet skal imidlertid gøre opmærksom på, at kravene til sikkerhedsforanstaltninger efter persondataloven og regler udstedt i medfør heraf går ud over de krav, der fremgår af forordningsforslagets artikel 26. Tilsynet finder derfor, at der kan være anledning til at præcisere forholdet mellem artikel 26 i forordningsforslaget og nationale regler fastsat på baggrund af databeskyttelsesdirektivet.

Forordningsforslagets artikel 26 fremstår ved gennemlæsning alene som en implementering af artikel 17, stk. 1, i direktiv 95/46/EF, hvorimod artikel 17, stk. 2, og 3, ikke er medtaget i forordningens bestemmelser.

3. Det fremgår af forslagets artikel 29, at medlemsstaterne fastsætter de sanktioner, der skal anvendes i tilfælde af overtrædelse af denne forordning med hensyn til databeskyttelse, og træffer alle nødvendige foranstaltninger til at sikre gennemførelsen heraf. Sanktionerne skal være effektive, stå i rimelig forhold til overtrædelsen og have en afskrækkende virkning. Medlemsstaterne giver senest på datoen for den meddelelse, som er omhandlet i artikel 37, stk. 1, Kommissionen meddelelse om disse bestemmelser, og enhver senere ændring meddeles omgående.

Datatilsynet kan hertil oplyse, at for så vidt angår behandlinger, som foretages *for private* pålægges der efter persondatalovens § 70, stk. 1, strafansvar for overtrædelse af en række af persondatalovens bestemmelser, undladelse af at efterkomme visse afgørelser truffet af Datatilsynet, for undladelse af at efterkomme tilsynets krav om enhver oplysning, der er af betydning for dets vir-

somhed, for at hindre tilsynet i at udøve sin inspektionsbeføjelse, for at tilsidesætte vilkår og lignende eller for at undlade at efterkomme forbud eller påbud.

I forbindelse med behandlinger, som foretages *for offentlige myndigheder*, er det fastsat, at der kan pålægges straf for overtrædelse af vilkår, som tilsynsmyndigheden har stillet i henhold til visse bestemmelser, jf. persondataloven § 70, stk. 2. Endvidere kan databehandlere pålægges straf for overtrædelse af lovens § 41, stk. 3, eller § 53. Strafansvar for andre overtrædelser af persondatalovens bestemmelser er således ikke fastlagt i persondatalovens regler, men vil efter omstændighederne kunne pålægges i medfør af straffelovens kapitel 16 om forbrydelser i offentlig tjeneste eller hverv m.v.

Datatilsynet finder på den baggrund, at det bør overvejes, om forslagets artikel 29 fordrer sanktioner, som ligger ud over reglerne i persondataloven og gældende dansk lovgivning i øvrigt.

4. Efter forslagets artikel 33, stk. 1, har enhver person i en medlemsstat ret til at anlægge sag ved eller indgive klage til de kompetente domstole i den pågældende medlemsstat, hvis han nægtes den ret til indsigt eller den ret til at få berigtiget eller slettet oplysninger om ham, som er omhandlet i artikel 31, stk. 1, og 2. Det følger endvidere af artikel 33, stk. 2, at de nationale tilsynsmyndigheders pligt til at bistå og på anmodning rådgive den pågældende i overensstemmelse med artikel 32, stk. 3, gælder under hele proceduren.

Efter persondatalovens § 58 påser Datatilsynet af egen drift eller efter klage fra en registreret, at behandlingen finder sted i overensstemmelse med loven og regler udstedt i medfør af loven. Datatilsynets opgave i forhold til borgerne består således i at behandle klager og i øvrigt vejlede om såvel konkrete som generelle spørgsmål inden for persondatalovens område, jf. herved også forvaltningslovens § 7.

Datatilsynet finder umiddelbart, at det giver anledning til tvivl, om artikel 33, stk. 2, indebærer en forpligtelse for tilsynet til at bistå en borger under et sagsanlæg ved domstolene. Efter Datatilsynets opfattelse ligger opgaver af denne karakter uden for tilsynets kompetence efter loven, og tilsynets ressourcemæssige situation giver heller ikke mulighed for at yde bistand og rådgivning i større omfang, jf. nedenfor under pkt. 5.

5. Med hensyn til Datatilsynets opgave som national tilsynsmyndighed skal tilsynet særligt gøre opmærksom på, at indførelsen af VIS-systemet må antages at medføre et øget behov for, at der foretages inspektioner bl.a. på danske ambassader og repræsentationer i udlandet. Hertil kommer behandlingen af eventuelle klagesager i forbindelse med danske myndigheders behandling af oplysninger i VIS.

Datatilsynet skal på denne baggrund understrege, at den bevillings- og personalemæssige situation ikke gør det muligt for tilsynet at påtage sig yderligere opgaver, uden at der samtidig tilføres de fornødne ressourcer til, eksempelvis

en udvidelse af inspektionsvirksomheden. Datatilsynet må derfor lægge afgørende vægt på, at tilsynets ressourcemæssige situation indgår i de videre overvejelser om VIS. I sin udtalelse af 3. november 2003 har Datatilsynet umiddelbart vurderet, at varetagelsen af funktionen som national tilsynsmyndighed vil belaste tilsynet på både løn- og driftssiden, og at et meget foreløbigt skøn er i størrelsesordenen 0,5 mio. kr. årligt. Tilsynet må derfor tage forbehold for en nærmere drøftelse i det videre forløb af spørgsmålet om ressourcer.

Med venlig hilsen

Janni Christoffersen
Direktør

DATATILSYNET

Justitsministeriet (22-50-79-15)
Slotsholmsgade 10
1216 København K

27. marts 2006

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-post
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2006-844-0048
Sagsbehandler
Anders Ankersfjerne
Direkte 3319 3238

Vedrørende Kommissionens forslag til rådsafgørelse om adgang til søgning i visuminformationssystemet (VIS) for myndigheder i medlemsstaterne, der har ansvaret for den indre sikkerhed, og for Europol med henblik på forebyggelse, afsløring og efterforskning af terrorhandlinger andre alvorlige strafbare handlinger (KOM(2005)600)

I breve af 9. februar og 2. marts 2006 har Justitsministeriet anmodet Datatilsynet om en udtalelse om ovennævnte forslag. Justitsministeriet har desuden fremsendt et grundnotat vedrørende forslaget.

Forslaget til rådsafgørelse har til formål at indføre det påkrævede retsgrundlag med hjemmel i afsnit VI i traktaten om den Europæiske Union (søjle 3) for at skabe grundlaget og fastsætte betingelserne for, at de myndigheder i medlemsstaterne, der har ansvaret for den indre sikkerhed,og Den Europæiske Politienhed (Europol) kan få adgang til visuminformationssystemet (VIS) med henblik på forebyggelse, afsløring og efterforskning af terrorhandlinger og de former for kriminalitet og de lovovertrædelser, der hører ind under Europols kompetenceområde i henhold til artikel 2 i Europol-konventionen ("alvorlige strafbare handlinger").

Forslaget skal ses i sammenhæng med Kommissionens forslag til Europa-Parlamentets og Rådets forordning om visuminformationssystemet (VIS) og udveksling af oplysninger mellem medlemsstaterne om visa til kortvarigt ophold (KOM(2004)835).

Det fremgår af det medsendte grundnotat, at VIS endnu ikke er i drift, og at der på nuværende tidspunkt ikke er fastsat nærmere, specifikke regler for danske myndigheders udveksling – gennem dette system – af visumoplysninger mv. med myndigheder i andre Schengen-lande.

Datatilsynet har tidligere afgivet to udtalelser om VIS-systemet, herunder til forslaget til forordning. Der henvises til brev af 3. november 2003 til Integrationsministeriet og brev af 31. januar 2005 til Ministeriet for Flygtninge, Indvandrer og Integration, som begge vedlægges i kopi.

Endvidere har artikel 29-arbejdsgruppen vedrørende databeskyttelse henholdsvis den 1. august 2004 og den 23. juni 2005 afgivet udtalelser om VIS. Senest har EDPS (den europæiske tilsynsførende for databeskyttelse) den 21.

januar 2006 afgivet en udtalelse vedrørende det foreliggende forslag til rådsafgørelse. Kopi vedlægges.

På det foreliggende grundlag har Datatilsynet umiddelbart nedenstående bemærkninger. Det bemærkes herved, at Datatilsynet ikke på nuværende tidspunkt har det fulde overblik over, hvorledes visuminformationssystemet i praksis vil blive implementeret i forhold til danske myndigheder.

1. Datatilsynet har gennem de seneste år fået forelagt en række initiativer, som viser en klar udvikling i retning af øget informationsudveksling og intensiveret samarbejde mellem retshåndhævende myndigheder, navnlig inden for Europa.

Datatilsynet har tidligere tilkendegivet, at tilsynet ser et bindende databeskyttelsesregelsæt som en afgørende forudsætning for udviklingen mod øget informationsudveksling på tredje søjle-området.

Datatilsynet har noteret sig, at det fremgår af artikel 8, stk. 1, i forslag til rådsafgørelse, at Rådets rammeafgørelse om beskyttelse af personoplysninger i forbindelse med det politimæssige og strafferetlige samarbejde finder anvendelse på rådsafgørelsen. Det fremgår endvidere, at behandlingen af personoplysninger overvåges af den uafhængige tilsynsmyndighed for databeskyttelse eller af de myndigheder, som er omhandlet i artikel 30 i den nævnte rammeafgørelsen.

Herudover foreslås det i forslagets artikel 8, stk. 4, at gruppen der er nedsat ved artikel 31 i Rådets rammeafgørelse om beskyttelse af personoplysninger i forbindelse med det politimæssige og strafferetlige samarbejde også udfører opgaver i relation til denne rådsafgørelse.

Datatilsynet skal imidlertid bemærke, at Rådets rammeafgørelse om beskyttelse af personoplysninger i forbindelse med det politimæssige og strafferetlige samarbejdepå nuværende tidspunkt ikke er vedtaget og at det præcise indhold derfor ikke kendes eller kan lægges til grund endnu. Datatilsynet skal i øvrigt henvise til tilsynets høringssvar af 17. marts 2006 om udkastet til denne rammeafgørelse.

Datatilsynet finder, at det må være en naturlig forudsætning, at et bindende databeskyttelsesregelsæt på 3. søjle-området vedtages, inden det foreliggende udkast til rådsafgørelse vedtages.

2. I forslagets artikel 2(e) er myndigheder, der har ansvaret for den indre sikkerhed funktionelt afgrænset, som de myndigheder i medlemsstaterne, der har ansvaret for forebyggelse, afsløring eller efterforskning af terrorhandlinger eller andre alvorlige strafbare handlinger.

Det fremgår af forslagets artikel 3, at de myndigheder, der har ansvaret for den indre sikkerhed, og som derved har tilladelse til at få adgang til VIS-data efter denne afgørelse, skal anføres i bilaget til afgørelsen.

Det fremgår ikke af de medsendte bilag eller det fremsendte grundnotat, hvilke danske myndigheder der har ansvaret for den indre sikkerhed, udover at der er tale om politimyndigheder.

Datatilsynet skal i den anledning henlede opmærksomheden på persondatalovens[1] anvendelsesområde.

Det fremgår af persondatalovens § 1, stk. 1, at loven gælder for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling, og for ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Det fremgår af persondatalovens § 2, stk. 4, 2. pkt., at bestemmelserne i lovens kapitel 8 og §§ 35-37 og § 39 ikke finder anvendelse på behandlinger, der foretages for politi og anklagemyndighed inden for det strafferetlige område.

Det fremgår endvidere af persondatalovens § 2, stk. 11, at loven ikke gælder for behandlinger, der udføres for politiets og forsvarets efterretningstjenester.

I det videre arbejde med forslaget til rådsafgørelse bør forholdet til persondatalovens anvendelsesområde således afklares og overvejes.

3. Forslagets artikel 5, 6 og 7 indeholder de nærmere betingelser for at få adgang til VIS-systemet for henholdsvis de myndigheder, der har ansvaret for den indre sikkerhed i de medlemsstater, som VIS-forordningen finder anvendelse på, og for de medlemsstater, som VIS-forordningen ikke finder anvendelse på samt for Europol.

I det omfang, der i henhold til forslaget til rådsafgørelse *indsamles og* videregives oplysninger inden for persondatalovens anvendelsesområde, skal Datatilsynet henlede opmærksomheden på persondatalovens regler om behandling, herunder videregivelse af oplysninger.

Det bemærkes i den forbindelse, at persondatalovens behandlingsregler indenfor lovens anvendelsesområde fortrænger reglerne om videregivelse i forvaltningslovens kapitel 8.[2]

Almindelige ikke-følsomme oplysninger kan, hvis det er *nødvendigt*, udveksles i forbindelse med konkret udøvelse af myndighedsopgaver i medfør af persondatalovens § 6.

---

[1] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger.

[2] Forholdet mellem forvaltningslovens videregivelsesregler og persondatalovens behandlingsregler er bl.a. nærmere beskrevet i Justitsministeriets vejledning af 12. november 2003 om offentlige myndigheders udveksling af personoplysninger som led i den koordinerede myndighedsindsats over for rockere-kriminalitet.

Ifølge lovens § 7, stk. 1, må der ikke behandles oplysninger om bl.a. racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning.

I lovens § 7, stk. 2 - 8, findes en række undtagelser til § 7, stk. 1. Bestemmelsen i stk. 1 finder f.eks. ikke anvendelse, hvis behandlingen er nødvendig af hensyn til en offentlig myndigheds varetagelse af sine opgaver på det strafferetlige område, jf. § 7, stk. 6.

Det følger af § 8, stk. 1, i persondataloven, at der for den offentlige forvaltning ikke må behandles oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i § 7, stk. 1, nævnte, medmindre det er nødvendigt for varetagelsen af myndighedens opgaver.

I medfør af § 8, stk. 2, må de i stk. 1 nævnte oplysninger ikke videregives. Videregivelse kan dog bl.a. ske, hvis videregivelsen sker til varetagelse af private eller offentlige interesser, der *klart* overstiger hensynet til de interesser, der begrunder hemmeligholdelse, herunder hensynet til den, oplysningen angår, jf. § 8, stk. 2, nr. 2. Videregivelsen kan endvidere ske, hvis videregivelsen er nødvendig for udførelsen af en myndigheds virksomhed eller påkrævet for en afgørelse, som myndigheden skal træffe, jf. § 8, stk. 2, nr. 3.

Endvidere fastsætter persondatalovens § 5 en række grundlæggende principper for behandling af personoplysninger, som altid skal være opfyldt, f.eks. krav om sagligt formål og proportionalitet.

Med hensyn til videregivelse fra VIS-systemet efter rådsafgørelsen, har Datatilsynet noteret sig, at videregivelsen sker på grundlag af en konkret vurdering. Der er således ikke tale om en ubegrænset, rutinemæssig adgang. Datatilsynet vurderer, at videregivelse af oplysninger fra VIS-systemet – efter en konkret vurdering i henhold til betingelserne i artikel 5, 6 og 7 i forslaget til rådsafgørelse – vil kunne ske inden for rammerne af persondatalovens behandlingsregler.

4. Forslagets artikel 10 pålægger Kommissionen, Europol og de nationale myndigheder pligt til at føre registre over alle behandlinger af oplysninger. Registrene skal vise det præcise formål med adgangen med henblik på søgning, datoen og tidspunktet for adgangen, de oplysninger, der er anvendt til søgningen, og de former for oplysninger, som der er søgt i, og navnet på den myndighed, der har fået adgang til og har søgt i oplysningerne.

Det fremgår endvidere, at registrene skal slettes efter en periode på et år efter udløbet af den femårige lagringsperiode, der er omhandlet i artikel 20, stk. 1, i VIS-forordningen, medmindre de nødvendige for kontrolprocedurer, som allerede er indledt.

Datatilsynet finder, at en effektiv kontrol med den korrekte behandling af personoplysninger ikke kun bør fokusere på transmissionens legalitet, men også på legaliteten af myndighedens adgang. Sidstnævnte gør det nødvendigt at logge eller dokumentere adgang til data.

Datatilsynet tilslutter sig således ønsket om registrering af enhver adgang til oplysningerne. En sådan registrering – eller logning – vil i Danmark skulle ske i en række tilfælde efter sikkerhedsbekendtgørelsen[3].

Det kan i den forbindelse oplyses, at Datatilsynet i forbindelse med forskellige tidligere initiativer på tredje søjle netop har understreget vigtigheden af, at man fra dansk side arbejder for at få bestemmelser om logning med i retsgrundlaget.

5. Som anført ovenfor fremgår det af forslagets artikel 8, stk. 1, at Rådets rammeafgørelse om beskyttelse af personoplysninger i forbindelse med det politimæssige og strafferetlige samarbejde finder anvendelse på rådsafgørelsen. Det fremgår endvidere, at behandlingen af personoplysninger overvåges af den uafhængige tilsynsmyndighed for databeskyttelse eller de myndigheder, som er omhandlet i artikel 30 i den nævnte rammeafgørelsen.

Det fremgår endvidere af artikel 8, stk. 6, at den eller de kompetente tilsynsmyndigheder for databeskyttelse mindst en gang om året undersøger lovligheden af behandlingen af personoplysninger efter denne afgørelse. De resulterende rapporter offentliggøres.

Datatilsynet har som nævnt ovenfor tidligere afgivet udtalelser om VIS-systemet. Datatilsynet henledte i disse udtalelser opmærksomheden på, at indførelsen af VIS-systemet må antages at medføre et øget behov for, at der foretages inspektioner bl.a. på danske ambassader og repræsentationer i udlandet. Hertil kommer behandlingen af eventuelle klagesager i forbindelse med danske myndigheders behandling af oplysninger i VIS.

Datatilsynet understregede på denne baggrund, at den bevillings- og personalemæssige situation ikke gør det muligt for tilsynet at påtage sig yderligere opgaver, uden at der samtidig tilføres de fornødne ressourcer til eksempelvis en udvidelse af inspektionsvirksomheden.

I sin udtalelse af 3. november 2003 har Datatilsynet umiddelbart vurderet, at varetagelsen af funktionen som national tilsynsmyndighed vil belaste tilsynet på både løn- og driftssiden, og at et meget foreløbigt skøn er i størrelsesordenen 0,5 mio. kr. årligt. Tilsynet tog derfor forbehold for en nærmere drøftelse i det videre forløb af spørgsmålet om ressourcer.

Datatilsynet formoder, at dele af - hvis ikke alle - de forudsatte yderligere tilsynsopgaver skal varetages af Datatilsynet. Datatilsynet skal i den forbindelse endvidere henvise til den vedtagte udtalelse fra EDPS, hvor der peges på at der er behov for et koordineret tilsyn med mindst et årligt møde mellem EDPS og alle de nationale tilsynsmyndigheder.

---

[3] Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000, som ændret ved bekendtgørelse nr. 200 af 22. marts 2000, om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for det offentlige forvaltning.

Datatilsynet må understrege, at en yderligere forøgelse af tilsynets opgaver vil nødvendiggøre tilførsel af flere ressourcer.

Med venlig hilsen

Janni Christoffersen
Direktør

Bilag: Kopi af Datatilsynets breve af 3. november 2003 til Integrationsministeriet og af 31. januar 2005 til Ministeriet for Flygtninge, Indvandrer og Integration
Kopi af udtalelse fra den Europæiske Tilsynsførende for Databeskyttelse (EDPS) om forslag til rådsafgørelse om adgang til søgning i visuminformationssystemet (VIS) for myndigheder i medlemsstaterne, der har ansvaret for den indre sikkerhed, og for Europol med henblik på forebyggelse, afsløring og efterforskning af terrorhandlinger andre alvorlige strafbare handlinger

DATATILSYNET

Ministeriet for Flygtninge, Indvandrere og Integration
Holbergsgade 6
1057 København K

Sendt til: dla@inm.dk

3. juli 2006

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-post
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2006-849-0098
Sagsbehandler
Camilla Sonne
Direkte 3319 3217

Vedrørende høring over Kommissionens forslag til Europa-Parlamentets og Rådets forordning om ændring af de fælles konsulære instrukser til de diplomatiske og konsulære repræsentationer - Deres 2004/4050-819

Ved e-post af 20. juni 2006 har Ministeriet for Flygtninge, Indvandrere og Integration anmodet om Datatilsynets eventuelle bemærkninger til Kommissionens forslag til Europa-Parlamentets og Rådets forordning om ændring af de fælles konsulære instrukser til de diplomatiske og konsulære repræsentationer med hensyn til indførelse af biometriske kendetegn, herunder bestemmelser om organisering af modtagelse og behandling af visumansøgninger med henblik på fastlæggelse af en dansk holdning og udarbejdelse af et grundnotat til Folketingets Europaudvalg.

1. Indledningsvis skal Datatilsynet henvise til de udtalelser, som tilsynet tidligere har afgivet om VIS-systemet i brev af 3. november 2003 til Integrationsministeriet og brev af 31. januar 2005 til Ministeriet for Flygtninge, Indvandrere og Integration.

2. I betragtning 7 i forslagets præambel er anført:
"Det er nødvendigt at indføre bestemmelser om situationer, hvor medlemsstaternes centrale myndigheder beslutter at outsource en del af visumhåndteringsprocessen til en ekstern tjenesteyder. Disse ordninger bør indføres under streng overholdelse af de generelle principper for udstedelse af visa og under overholdelse af databeskyttelseskravene i 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."

Datatilsynet skal hertil bemærke, at tilsynet som anført i tilsynets udtalelse af 31. januar 2005 forudsætter, at persondataloven og bekendtgørelser udstedt i medfør heraf gælder *inlår ud* for danske myndigheders behandling af oplysninger i forbindelse med VIS.

Tilsvarende må efter Datatilsynets opfattelse gøre sig gældende, når danske myndigheder som beskrevet i forordningsforslaget benytter en ekstern tjenesteyder som databehandler[1].

Datatilsynet forudsætter således, at de danske myndigheders benyttelse af en ekstern tjenesteyder skal ske under overholdelse af den danske persondatalov og regler udstedt i medfør heraf, herunder de sikkerhedskrav, der er fastsat i Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000, som ændret ved bekendtgørelse nr. 201 af 22. marts 2001, om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsbekendtgørelsen).

3. I forslaget er bl.a. anført (s.17), at:
"Den eller de pågældende medlemsstater skal indgå en kontrakt med den eksterne tjenesteyder i overensstemmelse med artikel 17 i direktiv 95/46. Inden den pågældende medlemsstats diplomatiske eller konsulære repræsentation indgår en sådan kontrakt, skal den inden for rammerne af det lokale konsulære samarbejde meddele de andre medlemsstaters diplomatiske og konsulære repræsentationer og Kommissionens delegation, hvorfor kontrakten er nødvendig.

Ud over de forpligtelser, som er fastsat i artikel 17 i direktiv 95/46, skal kontrakten også indeholde bestemmelser, der:
a) fastlægger tjenesteyderens nøjagtige ansvar
b) pålægger tjenesteyderen at handle efter anvisning fra de kompetente medlemsstater og kun at behandle oplysningerne med henblik på behandling af personoplysningerne i visumansøgningerne på vegne af de kompetente medlemsstater i overensstemmelse med direktiv 95/46
c) pålægger tjenesteyderen at give ansøgerne de oplysninger, som kræves i henhold til forordning ..... [udkastet til VIS-forordningen]
d) sikrer, at de konsulære medarbejdere når som helst kan få adgang til tjenesteyderens lokaler
e) pålægger tjenesteyderen at overholde fortrolighedsreglerne (herunder beskyttelse af de oplysninger, som indsamles i forbindelse med visumansøgninger)
f) indeholder en bestemmelse om suspension og ophør

Som nævnt forudsætter Datatilsynet, at de danske myndigheder skal iagttage persondataloven og bekendtgørelser udstedt i medfør heraf. De danske myndigheder skal således gennem en aftale med en ekstern tjenesteyder sikre sig, at persondataloven og sikkerhedsbekendtgørelsens iagttages.

Datatilsynet finder, at der kan være anledning til at præcisere forholdet mellem det i forordningen anførte om kravene til aftalen og de regler i national

---

[1] Persondatalovens § 3, nr. 5, definerer en databehandler som "En fysisk eller juridisk person, myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne."

lovgivning, der gennemfører databeskyttelsesdirektivet, som også indeholder krav om en aftale.

Efter Datatilsynets opfattelse kan det i den forbindelse overvejes at ændre formuleringen på side 17 i forslaget fra:

"Den eller de pågældende medlemsstater skal indgå en kontrakt med den eksterne tjenesteyder i overensstemmelse med artikel 17 i direktiv 95/46."

til

"Den eller de pågældende medlemsstater skal indgå en kontrakt med den eksterne tjenesteyder i overensstemmelse med de nationale regler fastsat til gennemførelse af artikel 17 i direktiv 95/46."

Ligeledes skal Datatilsynet foreslå, at det overvejes at ændre afsnittet derefter til:

"Ud over de forpligtelser, som er fastsat i de nationale regler, der gennemfører artikel 17 i direktiv 95/46, skal kontrakten også indeholde bestemmelser, der:"

Såfremt det måtte være hensigten, at denne forordning – eventuelt kombineret med forordningen om VIS – skal træde i stedet for nationale regler, der gennemfører artikel 17 i direktiv 85/46/EF, skal Datatilsynet bemærke, at fravigelsen af de sikkerhedskrav, der er fastsat i persondataloven og sikkerhedsbekendtgørelsen, eventuelt kan føre til en ringere retsstilling for de registrerede.

I givet fald må spørgsmålet om, hvorvidt der på dette område er behov for at etablere en anden ordning end persondataloven og en ordning, som eventuelt medfører en ringere retsbeskyttelse, efter Datatilsynets opfattelse bero på en politisk vurdering af, om vægtige samfundsmæssige hensyn taler herfor.

Det er derfor væsentligt, at spørgsmålet afklares og belyses i forbindelse med den videre behandling af forslaget.

Datatilsynet skal hermed også henvise til persondatalovens § 2, stk. 1, og forarbejderne hertil.

4. Ifølge forslaget (s. 19) forelægger medlemsstaterne Kommissionen de kontrakter, de indgår.

Det står ikke Datatilsynet klart, hvilken rolle Kommissionen i den forbindelse er tiltænkt i forhold til de sikkerhedskrav, der skal indgå i kontrakterne.

Den anvendte konstruktion aktualiserer efter Datatilsynet umiddelbare opfattelse det spørgsmål, som tilsynet har beskrevet ovenfor om forholdet til de nationale regler om datasikkerhed.

I forhold til de danske myndigheders databehandleraftaler må Datatilsynet forbeholde sig sin stillingtagen til disse som tilsynsmyndighed efter persondataloven.

5. I sit høringssvar af 31. januar 2005 har Datatilsynet under punkt 3 om sanktioner udtalt, at det bør overvejes, om forslaget til forordningen om VIS artikel 29 fordrer sanktioner, som ligger ud over persondataloven og gældende dansk lovgivning i øvrigt.

Anvendelsen af eksterne tjenesteydere må efter Datatilsynets umiddelbare opfattelse tages i betragtning i forbindelse med overvejelsen om behovet for sanktioner.

6. I sit høringssvar af 31. januar 2005 har Datatilsynet under punkt 5 understreget, at den bevillings- og personalemæssige situation ikke gør det muligt for tilsynet at påtage sig yderligere opgaver, uden at der samtidig tilføres de fornødne ressourcer til eksempelvis en udvidelse af inspektionsvirksomheden. Datatilsynet må derfor lægge afgørende vægt på, at tilsynets ressourcemæssige situation indgår i de videre overvejelser om VIS. I sin udtalelse af 3. november 2003 har Datatilsynet umiddelbart vurderet, at varetagelsen af funktionen som national tilsynsmyndighed vil belaste tilsynet på både løn- og driftssiden, og at et meget foreløbigt skøn er i størrelsesordenen 0,5 mio. kr. årligt. Tilsynet må derfor tage forbehold for en nærmere drøftelse i det videre forløb af spørgsmålet om ressourcer.

De forslag, der er indeholdt i det seneste udkast, formindsker ikke betydningen af Datatilsynets ressourcemæssige situation.

Med venlig hilsen

Lena Andersen
Kontorchef