



Den Digitale Taskforce
Christiansborg Slotsplads 1
1218 København K

Sendt til: strategi@tforce.dk

29. marts 2007

Vedrørende høring over udkast til strategi for digitalisering af den offentlige sektor 2007-2010

Datatilsynet
Borgergade 28, 5.
1300 København K

Den 19. marts 2007 er ovennævnte udkast til strategi offentliggjort på Den Digitale Taskforces hjemmeside www.modernisering.dk. Strategien er i offentlig høring frem til fredag den 13. april 2007.

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

I den anledning skal Datatilsynet udtale følgende:

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

1. Udveksling og genanvendelse af oplysninger

1.1. Det fremgår af den fremlagte strategi, at der skal sikres tværgående data-adgang mellem myndighederne (s. 6, 2. afsnit). Tilgængelige data på tværs af myndigheds- eller forvaltningsskel angives som en forudsætning for, at offentlige myndigheder kan levere en sammenhængende og nærværende service (s. 8, 3. afsnit).

J.nr. 2007-122-0025
Sagsbehandler
Christine Boeskov
Direkte 3319 3246

Videre fremgår det, at det er målsætningen, at borgere og virksomheder i videst muligt omfang kun skal aflevere oplysninger til det offentlige én gang. Det skal derfor sikres, at den offentlige sektor i så høj grad som muligt genbruger data på tværs af sektorer og myndighedsniveauer. I den forbindelse skal der sikres en bedre adgang til træk på fællesoffentlige nøgledata.

Som et af de initiativer, der skal sikre bedre digital service, er nævnt, at der i 2007 skal iværksættes analyser af potentialet og de juridiske udfordringer ved deling af registerdata og fælles drift af offentlige registre med henblik på at sikre genbrug af data i den offentlige sektor (s. 11, 2. afsnit, punkt 3).

1.2. Datatilsynet ser som udgangspunkt positivt på, at man anvender de teknologiske muligheder for effektivisering af det administrative arbejde. Datatilsynet kan således generelt tilslutte sig, at det er hensigtsmæssigt at søge at undgå, at de samme oplysninger skal indberettes flere gange til forskellige myndigheder.

Persondataloven¹ og databeskyttelsesdirektivet², som persondataloven gennemfører, sætter imidlertid grænser for myndighedernes udveksling og genbrug af oplysninger.

Datatilsynet har tidligere tilkendegivet, at persondatalovens begrænsninger navnlig ligger i kravet om, at offentlige myndigheder ikke må behandle eller have adgang til oplysninger, som de ikke har behov for i forbindelse med deres konkrete myndighedsudøvelse. Dette krav er udtrykt i forskellige afskygninger i lovens almindelige behandlingsregler, de generelle krav i lovens § 5 samt lovens regler om behandlingssikkerhed.

Almindelige, ikke-følsomme oplysninger kan i vidt omfang udveksles i forbindelse med *konkret* udøvelse af myndighedsopgaver i medfør af persondatalovens § 6.

Udveksling af følsomme oplysninger vil ligeledes i et vist omfang kunne ske *konkret* i medfør af persondatalovens §§ 7 og 8.

Persondatalovens § 5 indeholder en række grundlæggende principper for den dataansvarliges behandling, herunder indsamling, ajourføring, opbevaring m.v. af oplysninger. Disse krav skal altid være opfyldt.

Af persondatalovens § 5, stk. 2, følger, at indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål, og at senere behandling ikke må være uforenelig med disse formål (finalité-princippet).

Det bemærkes, at bestemmelsen ikke udelukker genbrug, udveksling mv. af oplysninger til andre formål end det eller de formål, hvortil oplysningerne er indsamlet af den dataansvarlige. Senere behandling af oplysningerne må blot ikke være *uforenelig* med de oprindelige formål.

Det følger endvidere af lovens § 5, stk. 3, 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.

1.3. Med hensyn til spørgsmålet om genanvendelse af personoplysninger skal Datatilsynet i øvrigt henlede opmærksomheden på artikel 29-gruppens³ udtalelse af 12. december 2003 vedrørende genanvendelse af oplysninger i offent-

¹ Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.

² Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

³ I henhold til artikel 29 i databeskyttelsesdirektivet er der nedsat en "gruppe vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger", den såkaldte "Artikel 29-gruppe". Gruppen er rådgivende og uafhængig og består af repræsentanter fra de nationale tilsynsmyndigheder.

lige myndigheders besiddelse – ‘Re-use of public sector information and the protection of personal data – striking the balance’ (WP 83).⁴

Dokumentet indeholder bl.a. en drøftelse af databeskyttelsesdirektivets anvendelighed på området samt, hvilke hensyn som skal inddrages ved en vurdering af, om f.eks. videregivelse er i overensstemmelse med finalitéprincippet.

Det nævnes bl.a. i den forbindelse, at hvor oplysningerne er afgivet på baggrund af en retlig forpligtelse, skal videregivelse vurderes særligt nøje under inddragelse af hensynet til ”reasonable expectations criterion”, dvs. hvad der med rimelighed må kunne forventes ved afgivelsen af oplysningerne.

Behovet for at tilvejebringe tekniske foranstaltninger til sikring af, at adgang til oplysningerne er begrænset eller struktureret på en sådan måde, at uberettiget behandling undgås, herunder f.eks. masseudtræk, understreges flere steder i dokumentet.

Det er endvidere anført, at hvor genanvendelse er lovhjemlet, bør denne også indeholde mulighed for, at der kan fremsættes indsigelse mod genanvendelse allerede på tidspunktet for indsamlingen af oplysningerne. Samtidig bør der gives meddelelse om denne retlighed.

2. Datasikkerhed

2.1. I et afsnit på s. 10 i strategien om sikker og tryk håndtering af data i den offentlige sektor er det bl.a. anført, at borgere og virksomheder generelt har stor tillid til den danske offentlige sektor. Det anføres videre, at det er afgørende, at denne tillid opretholdes og udbygges i forbindelse med den igangværende, gennemgribende digitalisering af det danske velfærdssamfund. Informationer og tjenester skal være tilgængelige og beskyttede, således at alle kan have tillid til, at de er korrekte, pålidelige og behandles med den fornødne fortrolighed.

Det anføres endvidere, at sikkerhed derfor skal integreres i den offentlige sektors it-arkitektur, og en fælles standard for håndtering af it-sikkerhed (DS484) skal udbredes til hele den offentlige sektor. Det skal ske på en sådan måde, at myndighederne fortsat kan give borgere og virksomheder en effektiv og sammenhængende service.

2.2. Datatilsynet skal gøre opmærksom på, at hensynet til beskyttelsen af oplysningerne om borgerne i Danmark ikke alene varetages ved den anførte standard, men tillige ved bl.a. persondataloven og de regler, bl.a. sikkerhedsbekendtgørelsen⁵, der er udstedt i medfør heraf.

⁴ Dokumentet kan ses på følgende adresse:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp83_da.pdf.

⁵ 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.

Datatilsynet undrer sig umiddelbart over, at dette regelsæt – der som nævnt bygger på et EU-direktiv – er uomtalt i udkastet til digitaliseringsstrategi.

I forlængelse af tilkendegivelsen om, at informationerne skal være tilgængelige og beskyttede, således at alle kan have tillid til, at de er korrekte, pålidelige og behandles med den fornødne fortrolighed, bør strategien efter Datatilsynets opfattelse indeholde en tilkendegivelse om, at den lovgivning, der sikrer dette, derfor selvsagt skal tages i betragtning ved digitaliseringen.

Persondatalovens regler må anses som så væsentlige i denne sammenhæng, at der på et tidligt tidspunkt i ethvert digitaliseringsprojekt bør indgå en vurdering af, hvordan løsningen udformes, således at loven og de hensyn, den varetager, tilgodeses.

Datatilsynet skal i den forbindelse tillige henviser til det grundlæggende princip om god databehandlingskik som nævnt i persondatalovens § 5, stk. 1. Princippet indebærer, at den dataansvarlige nøje skal overholde reglerne i loven, såvel i ånd som bogstav, og ikke må forsøge at omgå reglerne.

2.3. I den OECD-rapport, som omtales i strategien (s. 5) blev det om privacy bl.a. anført, at myndighederne anser emner som privatlivets fred og databeskyttelse som relativt mindre vigtige udfordringer ved implementering af digital forvaltning i Danmark, hvilket afspejler det stærke databeskyttelsesmiljø og det høje niveau af tillid blandt danskerne i relation til denne del af myndighedsudøvelsen. Dette skyldes til dels danskernes lange tradition for at afgive personoplysninger til en række offentlige registre, jf. s. 18 i rapporten.

Datatilsynet skal pege på, at selv om danskernes tillid generelt vurderes at være høj, er det efter tilsynets opfattelse stadig meget vigtigt, at de løsninger, der udformes, indeholder de elementer af databeskyttelse, der er nødvendige for, at borgerne fortsat kan bevare tilliden til de danske myndigheders behandling af deres personoplysninger – baseret på den entydige nøgle, som det danske personnummer udgør i praksis.

Digitaliseringen må således efter Datatilsynets opfattelse ikke ske på bekostning af databeskyttelsen. De begrænsninger, der følger af bl.a. persondataloven, må tages i betragtning, og løsningerne indrettes derefter.

2.4. Herudover vil det større flow af data, som synes at være en uundgåelig følge af digitaliseringen, aktualisere, at der overvejes nye mekanismer til beskyttelse af borgernes ret til privatliv. Herunder kan nævnes såkaldte privatlivsfremmende teknologier, der som supplement til de traditionelle datasikkerhedsinstrumenter kan medvirke hertil.

Datatilsynet skal i den forbindelse henlede opmærksomheden på, at Kommissionen i sin første beretning om gennemførelsen af databeskyttelsesdirektivet (95/46/EF) har peget på behovet for at opfordre regeringerne og den offentlige

sektor til at vise det gode eksempel ved at anvende privatlivsfremmende teknologier i deres egne behandlinger, f.eks. i forbindelse med digital forvaltning (e-government).⁶

3. Indsigtsret

3.1. I strategien er det anført, at borgernes og virksomhedernes tillid skal styrkes ved at give bedre mulighed for at få indsigt i deres egne sager og overblik over hele deres situation i forhold til det offentlige. Derfor skal borgere og virksomheder digitalt kunne følge med i behandlingen af deres egne sager og se, hvilke oplysninger der ligger til grund for sagen (s. 10, 9. afsnit).

3.2. Datatilsynet finder det positivt, at der gives borgerne adgang til egne sager og data. En sådan adgang er forudsat i forarbejderne til persondataloven.

I de tilfælde, hvor kun en del af myndighedens registrerede oplysninger om en borger er gjort digitalt tilgængelige, bør der efter Datatilsynets vurdering gøres tydeligt opmærksom herpå. Det vil endvidere være hensigtsmæssigt, at der samtidig gives oplysninger om, hvordan borgeren får indsigt i myndighedens øvrige oplysninger om vedkommende.

Datatilsynet skal endvidere gøre opmærksom på, at digital adgang til sager og data ikke nødvendigvis opfylder persondatalovens § 31, idet det af § 31, stk. 1, nr. 2-4, følger, at en person – udover meddelelse om, hvilke oplysninger der behandles – tillige har krav på meddelelse om behandlingens formål, kategorierne af modtagere af oplysninger samt tilgængelig information om, hvorfra disse oplysninger stammer.

Disse supplerende oplysninger vil ikke nødvendigvis fremgå ved den digitale adgang til egne sager og data, og myndighederne er således ikke i kraft af en digital løsning frigjort for deres forpligtelser efter persondatalovens § 31.

Det bemærkes, at der ikke kan stilles formkrav til en anmodning om indsigt efter persondataloven.

3.3. Retten til indsigt efter persondataloven omfatter alene oplysninger om den registrerede selv. Imødekommen af en anmodning om indsigt efter persondataloven kan ikke i sig selv begrunde videregivelse af oplysninger om andre, f.eks. andre sagsparter eller bipersoner, hvis betingelserne for videregivelse ikke er opfyldt. Dette vil forudsætte en konkret stillingtagen i de enkelte tilfælde.

3.4. For så vidt angår indsigt i myndigheders ESDH-systemer, skal Datatilsynet bemærke, at en meddelelse i henhold til persondatalovens § 31 tillige vil skulle indeholde en forklaring/oversættelse af de koder, som anvendes i det

⁶ First report on the implementation of the Data Protection Directive (95/46/EC), 15/05/2003, s. 25.

pågældende ESDH-system, og som borgerne normalt ikke vil forventes at kunne forstå.

Datatilsynet går ud fra, at der ikke i alle tilfælde vil skulle gives adgang til alle de oplysninger, som en myndighed behandler om en borger, f.eks. ikke til myndighedens udkast eller interne arbejdsdokumenter. Såvel forvaltningsloven som offentlighedsloven indeholder imidlertid bestemmelser, hvorefter der i en række tilfælde alligevel vil være ret til aktindsigt i myndighedens interne arbejdsdokumenter.

I forhold til indsichtsretten efter persondataloven vil der herudover være mulighed for efter en konkret vurdering at undtage oplysninger fra indsigt, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til private eller offentlige interesser, jf. persondatalovens § 32, stk. 1, jf. § 30.

Datatilsynet skal påpege, at muligheden for, at borgerne kan ”følge med” i deres sager, vil forudsætte, at der løbende foretages konkrete vurderinger i forhold til de oplysninger, der er under behandling, med henblik på at fastlægge, hvorvidt borgerne kan få indsigt. Efter Datatilsynets opfattelse må det derfor forventes, at en sådan indsichtsadgang vil være ganske ressourcekrævende.

For Datatilsynets eget vedkommende finder tilsynet ikke – inden for sine nuværende rammer – at kunne afsætte ressourcer til på forhånd at foretage vurderinger af, hvilke oplysninger der kan gives indsigt i, i samtlige sine sager.

Det kan i øvrigt oplyses, at der efter persondatalovens § 31 ikke er ret til indsigt i den sikkerhedslog, som offentlige myndigheders systemer i et vist omfang skal indeholde, og hvori der registreres oplysninger om, bl.a. hvilken bruger der har anvendt personoplysningerne.⁷

4. Selvbetjening via borgerportalen

4.1. Det fremgår af strategien, at alle digitale selvbetjeningsløsninger i 2010 bør integreres fuldt ud i borgerportalen, og at borgerportalen i 2012 skal være fuldt udviklet med alle digitale selvbetjeningsløsninger fuldt integreret (s. 11. afsnit 1, punkt 3).

4.2. Som udbyder af en digital selvbetjeningsløsning (Datatilsynets elektroniske anmeldelsessystem)⁸ skal Datatilsynet påpege, at også denne del af strategien har konsekvenser for tilsynet.

⁷ Efter sikkerhedsbekendtgørelsens § 19 skal der foretages maskinel registrering (logning) af de anvendelser af personoplysninger, som er omfattet af offentlige myndigheders anmeldelsespligt til Datatilsynet. Det vil navnlig sige behandling af fortrolige og følsomme personoplysninger.

⁸ Hovedparten af de anmeldelser, der efter persondataloven skal indgives til Datatilsynet, kan indsendes elektronisk via tilsynets hjemmeside. Offentlige myndigheders anmeldelser modtager Datatilsynet efter eDag2 som udgangspunkt kun i elektronisk form.

Tilsynets elektroniske anmeldelsessystem indeholder faciliteter, som ikke umiddelbart vil kunne integreres i en portal. Tilsynet tilbyder funktioner, som indebærer, at en allerede behandlet anmeldelse kan benyttes som kladde for en anden anmeldelse. På visse områder, f.eks. private virksomheders personaleadministration, kontaktbureauer og alternative behandlere, har Datatilsynet udarbejdet skabeloner til anmeldelser. Endvidere kan der i tilsynets anmeldelsessystem oprettes udkastkonti, hvor udkast til anmeldelser kan gemmes med henblik på færdiggørelse på et senere tidspunkt. Desuden indeholder tilsynets hjemmeside en ordbogsfunktion, hvor betydningen af bl.a. begreber, som har betydning for anmeldelsespligten, forklares.

Sådanne services risikerer at gå tabt, hvis Datatilsynets system skal integreres med portalløsninger. Funktionerne er udarbejdet dels for at gøre det lettere for myndigheder og private at foretage anmeldelse til Datatilsynet, dels for at lette Datatilsynets arbejde med behandlingen af anmeldelserne. Anvendelse af portalløsninger, der ikke understøtter disse funktioner, medfører, at den effektivisering, som er tilstregtet og opnået med f.eks. sådanne funktioner, mistes.

Datatilsynets egen erfaring med portalen virk.dk er, at tilsynets funktioner ikke er integreret i portalen.

4.3. Datatilsynet skal i øvrigt understrege vigtigheden af, at der skabes gennemsigtighed på portaler, således at det altid fremgår tydeligt, hvem borgeren eller virksomheden kommunikerer med.

5. Kopi af dette brev er sendt til Justitsministeriets Budget- og planlægningskontor.

Med venlig hilsen

Janni Christoffersen
Direktør