Indenrigs- og Sundhedsministeriet
Dato: 11. april 2005
Kontor: 2.k.kt.
J.nr.: 2004-2200-21
Sagsbeh.: abt
Fil-navn: LKS/FT.beh./Spm1.KOU.L72.svar

Besvarelse af spørgsmål nr. 1 (L 72), som Folketingets Kommunaludvalg har stillet til indenrigs- og sundhedsministeren den 10. marts 2005

Spørgsmål 1:

"Ministeren bedes redegøre for, hvordan ministeren har tænkt sig, at borgerservicecentrene skal fungere i praksis. Skal de ansatte i borgerservicecentrene have adgang til alle de offentlige registre, som de kan tænkes at skulle bruge oplysninger fra. Eller skal de ansatte, når de står med en konkret borger og en konkret sag, først anmode om adgang og begrunde, hvorfor adgang er nødvendig eller har de adgang men først skal igennem en procedure, hvor de f.eks. skriftligt skal notere, hvorfor de skal bruge oplysningerne."

Svar:

Kommunerne træffer selv beslutning om deres praktiske arbejdstilrettelæggelse. Det gælder på alle forvaltningsområder, også i forhold til borgerservicecentre. Jeg kan derfor ikke bestemme, hvordan borgerservicecentrene i praksis skal fungere. Kommunernes fastlæggelse af arbejdstilrettelæggelsen skal imidlertid ske inden for rammerne af gældende regler og praksis, som i relation til adgang til elektroniske systemer og muligheden for f.eks. i forbindelse med opslag at foretage samkøring m.v. indeholder en relativt detaljeret regulering af disse spørgsmål.

Der gælder således en række sikkerhedsregler i relation til offentlige myndigheders elektroniske behandling af personoplysninger. Endvidere gælder der særlige regler i relation til samkøring eller sammenstilling af personoplysninger i kontroløjemed. Disse regler gælder for alle dele af den offentlige forvaltning, herunder for borgerservicecentre.

Reglerne fremgår dels af lov om behandling af personoplysninger (persondataloven), dels af bekendtgørelse nr. 528 af 15. juni 2000 som ændret ved bekendtgørelse nr. 201 af 22. marts 2001 om sikkerhedsforanstaltninger i forbindelse med offentlige myndigheders behandling af personoplysninger (sikkerhedsbekendtgørelsen).

Forslaget til lov om kommunale borgerservicecentre ændrer ikke de persondataretlige sikkerhedsregler eller reglerne i relation til samkøring i kontroløjemed. Der henvises til lovforslagets almindelige bemærkninger, afsnit 4.3.1.3.

De persondataretlige sikkerhedsregler og reglerne i relation til samkøring i kontroløjemed henhører under Justitsministeriet. Besvarelsen er derfor afstemt med Datatilsynet.

Nedenfor er nævnt en række persondataretlige sikkerhedsregler, som fremgår af gældende regler og praksis. Jeg forudsætter, at kommunerne i praksis overholder gældende regler og praksis.

Herudover har Datatilsynet givet udtryk for, at brugen af medarbejdere til løsning af forskellige opgaver gør det påkrævet, at der i forbindelse med borgerservicecenterkonstruktionen sker en *forøgelse af behandlingssikkerheden*, herunder med hensyn til styring af brugerrettigheder og interne kontrolordninger i forhold til medarbejdernes anvendelse af IT-systemerne. I det omfang der fastsættes supplerende sikkerhedsregler vedrørende forøgelse af behandlingssikkerheden i borgerservicecentrene, eller i det omfang Datatilsynet udvikler en praksis med hensyn til niveauet og indholdet af de tiltag, som er nødvendige for at forøge behandlingssikkerheden i borgerservicecentrene, må det forudsættes, at kommunerne ligeledes i praksis vil overholde sådanne regler eller praksis.

Der kan vedrørende de gældende regler og praksis samt Datatilsynets tilkendegivelser om fremtidige regler og praksis oplyses følgende:

1. Adgang til elektroniske systemer

Efter persondatalovens § 5, stk. 1, skal personoplysninger behandles i overensstemmelse med god databehandlingsskik. Efter lovens § 41, stk. 3, skal den dataansvarlige bl.a. træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Endvidere er der fastsat regler om autorisation i sikkerhedsbekendtgørelsens § 11, stk. 1 og 2. Efter disse bestemmelser må kun personer, som autoriseres hertil, have adgang til de personoplysninger, der behandles, og der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for. Der gælder med andre ord et krav om sagligt behov for adgang til personoplysningerne.

En adgang for en enkelt kommunal medarbejder til alle borgerrelaterede oplysninger kan være vanskelig at forene med persondatalovens § 5 og de generelle krav om datasikkerhed i lovens § 41, stk. 3, og sikkerhedsbekendtgørelsens § 11. Dette uanset, at en medarbejder med en sådan generel adgang tilsvarende varetager en lang række opgaver, som hver for sig sagligt berettiger til adgang til de enkelte oplysninger.

Der henvises til lovforslagets almindelige bemærkninger, afsnit 4.3.1.3.

I relation til ***kommunens egne systemer*** indebærer reglerne, at medarbejderne i borgerservicecentrene ikke må autoriseres til, f.eks. ved blot at ind-

taste personnummeret på en borger, at få adgang til samtlige oplysninger i kommunen vedrørende borgeren, uanset om medarbejderen teoretisk kan tænkes at have brug for oplysningerne eller ej. Indenrigs- og Sundhedsministeriet bekendt findes sådanne systemer i øvrigt ikke. Herudover må en medarbejder ikke autoriseres til at have adgang til alle de offentlige registre, som medarbejderen teoretisk kan tænkes at skulle bruge oplysninger fra. Navnlig for så vidt angår elektroniske registre og andre elektroniske systemer med følsomme oplysninger / sociale oplysninger, må kommunerne afstå fra at give adgang til medarbejdere, som kun forholdsvis sjældent vil have brug for oplysningerne.

Behovet for adgang til systemerne må vurderes konkret og individuelt i forhold til den enkelte medarbejder og dennes arbejdsopgaver.

For brugere, som ikke længere har behov for de autorisationer, de har fået udstedt, skal autorisationerne inddrages. Det gælder f.eks. medarbejdere, som flytter til andet arbejdsområde. Der henvises til Datatilsynets vejledning nr. 37 af 2. april 2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsvejledningen), ad § 11, stk. 2. Endvidere skal kommunen i forhold til anmeldelsespligtige systemer (systemer med fortrolige, herunder følsomme, oplysninger er som udgangspunkt anmeldelsespligtige) mindst en gang hver halve år sikre sig, at de autoriserede personer fortsat opfylder autorisationsbetingelserne. Der henvises til sikkerhedsbekendtgørelsens § 17.

Kommunerne skal fastsætte nærmere interne bestemmelser om sikkerhedsforanstaltninger (uddybende sikkerhedsregler) til uddybning af de regler, som fremgår af sikkerhedsbekendtgørelsen. Bestemmelserne skal bl.a. omfatte administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer. Der henvises til sikkerhedsbekendtgørelsen § 5, stk. 1.

Lovforslagets videregivelsesregler, jf. lovforslagets § 3, stk. 1, og § 3, stk. 1, jf. stk. 6, giver ikke borgerservicecentrene et krav på terminaladgang til ***andre myndigheders systemer***. En sådan terminaladgang kan navnlig være relevant, hvis borgerservicecentrene udfører myndighedsudøvelse på vegne af andre myndigheder. Lovforslaget giver ikke hjemmel til overladelse af myndighedsudøvelse til kommunerne. Der henvises i den forbindelse til besvarelsen af spørgsmål 4. En terminaladgang til en anden myndigheds systemer kan også være relevant, hvis en opgave i lovgivningen er delt mellem kommunen og den pågældende myndighed, f.eks. for så vidt angår pas- og kørekortområdet. Der henvises i den forbindelse til besvarelsen af spørgsmål 7, eksempel 3.

I hvilket omfang en *videregivelse* af oplysninger, som sker i forbindelse med en evt. terminaladgang, vil være lovlig, afhænger ikke af de persondataretlige sikkerhedsregler, men af de videregivelsesregler, som gælder på det pågældende område. Datatilsynet har i øvrigt oplyst, at det endnu ikke

Datatilsynet bekendt er afklaret, i hvilket omfang og på hvilke vilkår borgerservicecentre vil kunne få adgang til andre myndigheders edb-systemer med personoplysninger, ligesom det på nuværende tidspunkt er uafklaret, om der bliver tale om at supplere adgangskontrol og autorisationsordninger med andre løsninger. En løsning, hvor det noteres i systemet, hvorfor der foretages opslag, må i disse tilfælde antages at medvirke til at sikre, at der kun behandles oplysninger, når det er nødvendigt.

2. Øget behov for sikkerhedskontrol, uddannelse m.v.

Datatilsynets har oplyst, at brugen af medarbejdere til løsning af forskellige opgaver gør det påkrævet, at der i forbindelse med servicecenterkonstruktionen og IT-understøttelsen af centrene sker en forøgelse af behandlingssikkerheden, herunder med hensyn til ***styring af brugerrettigheder***. En sådan styrkelse kan ske på forskellig vis. Datatilsynet har peget på følgende muligheder, idet Datatilsynet har understreget, at der næppe er tale om en udtømmende oversigt over, hvorledes brugerrettigheder kan styres:

- Først og fremmest er det vigtigt, at tildelingen af brugerrettigheder håndteres forsvarligt i den enkelte myndighed. Der skal være fastlagt en formel autorisationsprocedure- og arbejdsgang. Heri skal indgå, at der forud for tildelingen af autorisation foretages en vurdering af, hvad den enkelte bruger har behov for at være autoriseret til. Vurderingen og godkendelsen heraf skal foretages på funktionsniveau og af den pågældendes funktionschef.

- Herudover kan der være behov for at etablere tekniske løsninger, der begrænser brugernes adgang til de oplysninger, der er nødvendige. En simpel løsning kan være koder, der kan anvendes til at begrænse adgangen til en konkret sag eller gruppe af sager.

- I en række systemer sker der en teknisk afgrænsning af brugerens adgang ud fra en række kriterier. F.eks. begrænses adgangen til det fælles datagrundlag, der anvendes i Arbejdsmarkedsportalen, ud fra geografiske, tidsmæssige og opgavemæssige hensyn (jf. forslag til lov om ansvaret for og styringen af den aktive beskæftigelsesindsats – L 22).

- Begrænsningen af adgangen til personoplysninger ud fra geografiske hensyn finder i praksis sted i en række systemer, således at den enkelte myndighed kun har adgang til oplysninger om personer, hvor dette er relevant i forhold til det geografiske område, som myndigheden dækker.

- Begrænsninger i adgangen ud fra tids- og opgavemæssige hensyn kan f.eks. ske ved, at der kun etableres adgang til de oplysninger, som er nødvendige i forhold til opgaver, myndigheden varetager, og kun så længe myndighedens opgaver begrunder adgang. Dette vil

formentlig kunne være relevant i forhold til kommunernes adgang til andre myndigheders systemer.

Inden for myndigheden skal den enkelte medarbejders adgang ligeledes fastlægges i forhold til de behov, som medarbejderen har i forbindelse med de forskellige arbejdsopgaver, som han eller hun varetager.

Sagsbehandlingssystemer, der automatisk henter oplysninger i forskellige systemer, skal søges indrettet således, at der kun indhentes oplysninger, som er nødvendige i den pågældende sag. Hvilke oplysninger, der skal indhentes, kan evt. fastlægges i forhold til forskellige typer af ensartede sager.

- Herudover kan det overvejes, om adgangen til oplysninger om en borger kan tilrettelægges således, at et kort, som borgeren har i sin besiddelse, skal aflæses, før end medarbejderen hos myndigheden får adgang til oplysninger om borgeren.

  Datatilsynet har i den forbindelse henledt opmærksomheden på, at Rådet for IT-Sikkerhed i sin årsberetning for 2004 har anført, at Rådet mener, at den digitale signatur skal videreudvikles hen mod et egentligt chipkort eller lignende til alle borgere. Kortet bør kunne bruges af ejeren overalt i det danske samfund.

Datatilsynet har endvidere oplyst, at brugen af medarbejdere til løsning af forskellige opgaver gør det påkrævet, at der i forbindelse med servicecenterkonstruktionen og IT-understøttelsen af centrene sker en forøgelse af behandlingssikkerheden med hensyn til ***interne kontrolordninger***.

Med interne kontrolordninger sigtes f.eks. til muligheden for, at kommunerne foretager stikprøvevis kontrol af loggen i systemer med følsomme oplysninger; dels af præventive hensyn, dels med henblik på at opdage og undersøge eventuelt misbrug af adgang.

Datatilsynet har herudover oplyst, at det herudover også er relevant at overveje andre ordninger. En løsning, hvor det noteres i systemet, hvorfor der foretages opslag, kan efter Datatilsynets opfattelse medvirke til at sikre, at der kun behandles oplysninger, når det er nødvendigt. En lignende løsning anvendes i systemer på sundhedsområdet, hvor det registreres i systemet f.eks. i form af en tro og love erklæring, at der er givet samtykke, eller at den pågældende sundhedsperson har den registrerede person i behandling.

Herudover gør brugen af medarbejdere til løsning af forskellige opgaver det påkrævet, at der i forbindelse med borgerservicecenterkonstruktionen og IT-understøttelsen af centrene er ***fokus på uddannelse og vejledning af medarbejderne*** om behandling af personoplysninger.

Der henvises til lovforslagets almindelige bemærkninger, afsnit 4.3.1.3.

3. Samkøring i kontroløjemed

Særligt med hensyn til medarbejdernes adgang til at samkøre oplysninger i de systemer, som de har adgang til, kan oplyses følgende:

Med samkøring sigtes til forskellige tekniske løsninger, hvorved der sker en sammenkobling af oplysninger, som kommer fra elektroniske systemer, der er oparbejdet med henblik på forskellige formål. Navnlig samkøring, hvorved der dannes et nyt system, som indeholder andre datatyper end de oprindelige systemer, eller hvorved de eksisterende oplysninger gøres tilgængelige i nye sammenhænge, har påkaldt sig interesse i persondataretten. Der henvises til betænkning nr. 1345 / 1997 om behandling af personoplysninger, s. 67 – 68.

Der gælder efter persondataloven et krav om, at samkøring eller sammenstilling i kontroløjemed kun må finde sted, såfremt der forinden er indhentet en tilladelse fra Datatilsynet, jf. lovens § 45, stk. 1, nr. 4

Herudover gælder en række materielle krav i relation til samkøring i kontroløjemed. Retsudvalgets flertal gav således i betænkning over lovforslag nr. L 50 af 16. januar 1991 udtryk for, hvilke betingelser der efter flertallets opfattelse skulle være opfyldt, såfremt offentlige myndigheder ville foretage samkøring af registre, som indeholder fortrolige, herunder følsomme, personoplysninger. Registertilsynets, og senere Datatilsynets, praksis, som er udviklet på grundlag af disse tilkendegivelser, kan sammenfattes således: Samkøring i kontroløjemed kun kan finde sted, såfremt det sker på et klart og utvetydigt retsgrundlag, hvilket i praksis vil sige på grundlag af direkte lovhjemmel. De berørte personer skal endvidere have fået meddelelse om kontrollen, inden de afgiver oplysninger til myndigheden. Endelig bør forudgående kontrol, det vil sige den kontrol, som myndighederne iværksætter, før der træffes afgørelse i en sag, så vidt muligt anvendes frem for kontrol, der først iværksættes, efter at afgørelsen er truffet.

Disse regler ændres som nævnt ovenfor ikke af forslaget til lov om kommunale borgerservicecentre. De gælder således ligeledes for medarbejdere i såvel nuværende som fremtidige borgerservicecentre.