Datasikkerhed i borgerservicecentre

Regler og praksis

Til it-medarbejderne, sikkerhedsmedarbejderne og ledelsen

Datasikkerhed i borgerservicecentre
Regler og praksis
Til it-medarbejderne, sikkerhedsmedarbejderne og ledelsen

Udarbejdet af Projektgruppen om Bedre Borgerbetjening (projektgruppe bestående af medlemmer fra Indenrigs- og Sundhedsministeriet og KL) og Datatilsynet

Udgivet af:
Indenrigs- og Sundhedsministeriet
Slotsholmsgade 10-12
1216 København K
Telefon: 72 26 90 00
Telefax: 72 26 90 01
E-post: im@im.dk

KL
Weidekampsgade 10
Postboks 3370
2300 København S
Telefon: 33 70 33 70
Telefax: 33 70 33 71
E-post: kl@kl.dk

Datatilsynet
Borgergade 28, 5.
1300 København K
Telefon: 33 19 32 00
Telefax: 33 19 32 18
E-post: dt@datatilsynet.dk

Grafisk design:
Indenrigs- og Sundhedsministeriet

Udgivelsesår: 2006

Publikationen er alene offentliggjort elektronisk

ISBN 87-7601-183-6 (elektronisk udgave)
Version: 1.0
Versionsdato: 20. september 2006
Publikationen er tilgængelig på http://www.im.dk,
http://www.kl.dk/datasikkerhed og
http://www.datatilsynet.dk

Indholdsfortegnelse

Om publikationen

Borgerservicecenteret er et af kommunens vigtigste ansigter udadtil. Det besøges af mange af kommunens borgere – og mange borgere besøger kun denne del af den kommunale administration.

Der passerer et stort antal personoplysninger igennem borgerservicecenteret. Der er mange henvendelser, og medarbejderne har ofte på grund af deres brede opgavesammensætning adgang til flere it-systemer med personoplysninger end kommunale medarbejdere, som arbejder med mere afgrænsede opgaver. Desuden er der tit mange medarbejdere og borgere i borgerservicecenterets lokaler, hvilket skal ses i sammenhæng med, at der også printes eller kopieres papirer med personoplysninger.

Det er af stor betydning for borgerne, at oplysninger om dem behandles på en betryggende måde, og datasikkerheden er en vigtig parameter for, om borgerne oplever borgerservicecenteret som et trygt sted at henvende sig.

Hvad er et borgerservicecenter?
Et borgerservicecenter er en enhed, der løser forskellige administrative borgerbetjeningsopgaver (f.eks. vejviserfunktioner, udlevering og modtagelse af blanketter, behandling af ansøgningssager m.v.). Et borgerservicecenter betjener borgere, der møder fysisk frem. Borgerservicecenteret kan også derudover yde borgerbetjening ad andre kanaler, f.eks. telefonbetjening og besvarelse af breve og e-post. Den form for borgerbetjening er i så fald også en del af borgerservicecenteret. Et borgerservicecenter varetager typisk flere opgaveområder og kan ofte give en mere bred betjening af borgere, som befinder sig i en livssituation, hvor der er behov for hjælp og vejledning inden for flere forskellige af kommunens fagområder (f.eks. en borger, som har fået et barn, eller som flytter til kommunen).

Et borgerservicecenter er typisk beliggende et bestemt sted, men mobile enheder vil også kunne være et borgerservicecenter. Det er uden betydning, hvad centeret kaldes, og hvordan det er organiseret.

Derfor må der tages særlig højde for datasikkerheden i forbindelse med IT-understøttelsen af borgerservicecentrene. I persondataloven og sikkerhedsbekendtgørelsen er der fastsat regler om datasikkerhed. Det er regler, der gælder generelt i forhold til alle it-systemer med personoplysninger i hele kommunen og dermed også borgerservicecentrene. Reglerne er beskrevet i sikkerhedsvejledningen. Derudover er der enkelte særlige sikkerhedsregler, der kun gælder for borgerservicecentrene.

Denne publikation er skrevet til kommunens it-medarbejdere, sikkerhedsmedarbejdere (dvs. medarbejdere, der indgår i kommunens sikkerhedsorganisation) og lederne af borgerservicecentrene og beskriver de datasikkerhedsregler, der er særligt relevante i forhold til borgerservicecentrene.

Læs om:

- **Hvordan skal it-systemerne indrettes?** (kapitel 1)
- **Hvordan skal edb-udstyr og lign. placeres?** (kapitel 2)
- **Hvem må have adgang til it-systemerne?** (kapitel 3)
- **Hvordan skal medarbejderne instrueres om datasikkerhed?** (kapitel 4)
- **Valg og administration af kontrolordninger** (kapitel 5)
- **Datatilsynets kontrol med datasikkerheden** (kapitel 6)

Publikationen er et sammendrag af de sikkerhedsregler i persondataloven, sikkerhedsbekendtgørelsen og sikkerhedsvejledningen, der har størst betydning for borgerservicecentrene. Publikationen giver også svar på, hvilke sikkerhedsforanstaltninger der kræves for at imødekomme Datatilsynets tilkendegivelser om, at datasikkerheden bør være skærpet i borgerservicecentrene. I hvert afsnit er det nævnt, om reglerne gælder hele kommunen eller kun for borgerservicecentre.

Publikationen er blevet til i et samarbejde mellem Datatilsynet, Indenrigs- og Sundhedsministeriet og KL. Publikationen kan findes på www.datatilsynet.dk, www.im.dk og www.kl.dk/datasikkerhed.

Persondataloven: Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger
http://www.datatilsynet.dk/lovgivning/personoplysninger/indhold.asp
Sikkerhedsbekendtgørelsen: Bekendtgørelse nr. 528 af 15. juni 2000
http://www.datatilsynet.dk/include/show.article.asp?art_id=495&sub_url=/lovgivning/indhold.asp
Sikkerhedsvejledningen: 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
http://www.datatilsynet.dk/include/show.article.asp?art_id=502&sub_url=/lovgivning/indhold.asp

1. Hvordan skal it-systemerne indrettes?

1.1. Teknisk adgangskontrol og opsætning af rettigheder

Adgang kræver password eller lign.

It-systemer med personoplysninger skal indrettes sådan, at det ikke er teknisk muligt at få adgang til it-systemerne uden brugeridentifikation og et password eller lignende sikkerhedsløsning[1].

Det skyldes, at personoplysninger i it-systemer ikke må komme til uvedkommendes kendskab[2]. Kun den borger, som oplysningerne omhandler, samt den eller de medarbejdere, der behandler den pågældende type sager, må som udgangspunkt gives adgang til borgerens personoplysninger. Øvrige borgere og andre uden for kommunens forvaltning er normalt uvedkommende. Men også kommunale medarbejdere er "uvedkommende", hvis de ikke har konkret brug for oplysningerne for at løse deres arbejdsopgaver. Derfor må kun personer, som autoriseres til det, have adgang til personoplysninger i kommunens it-systemer.

Kravet om teknisk adgangskontrol gælder for alle it-systemer med personoplysninger, uanset der kun er tale om ikke-fortrolige personoplysninger. Kravet gælder for alle typer af it-systemer; ikke kun egentlige databaser, men også sagsbehandlingssystemer, e-postsystemer, ESDH-systemer, journalsystemer osv.

Selvom et system ikke indeholder personoplysninger, kan det også i nogle tilfælde være hensigtsmæssigt at etablere teknisk adgangskontrol, hvis systemet indeholder fortrolige oplysninger om virksomheder, foreninger og lign.

It-systemer til flere forskellige opgaver

Hvis samme it-system bruges til flere forskellige opgaver, skal medarbejderne i it-systemet kunne tildeles rettigheder til netop de oplysninger i systemet, som vedrører de opgaver, han eller hun beskæftiger sig med. Det er navnlig relevant i forhold til f.eks. ESDH-systemer, tekstbehandlingssystemer, e-postsystemer og andre systemer, som bruges på tværs af forskellige kommunale opgaver.

Hvorfor differentieret adgang?

Ved at opdele adgangen til de relevante sager eller oplysninger kan kommunen sikre, at oplysninger om borgerne (heriblandt fortrolige eller følsomme oplysninger) ikke kan ses af medarbejdere, som ikke har brug for oplysningerne.

---

[1] Jf. § 12 i sikkerhedsbekendtgørelsen

[2] Jf. § 5, stk. 1, og § 41, stk. 3, i persondataloven

Adgang til sager

En løsning kan være at indrette it-systemerne sådan, at *bestemte, konkrete sager eller en gruppe af sager* kan tildeles en særlig kode, og at medarbejderne kan tildeles rettigheder til adgang til bestemte koder. Det er derfor en god idé at oprette sager efter enkeltsagsprincippet, så f.eks. flere forskellige sagsforhold vedrørende den samme borger ikke ligger på samme journalnummer / sag.

Eksempelboks 1:
Medarbejdere i boligstøttesektionen gives rettigheder til adgang til boligstøttesagerne i ESDH-systemet.

Adgang til oplysninger

Det kan eventuelt også være relevant at indrette it-systemerne sådan, at der kan gives rettigheder til at slå op på et bestemt *niveau* (f.eks. kun oplysninger om, at der findes en bestemt sag, men ikke de underliggende dokumenter i sagen) eller bestemte *typer af oplysninger*. Nogle sager har dog en så følsom karakter, at kun de medarbejdere, der konkret behandler den type sager, må vide, at sagerne overhovedet findes.

Eksempelboks 2:
Medarbejdere, hvis opgave er at vejlede borgere, der befinder sig i en almindeligt forekommende livssituation – f.eks. en borger, der sammen med sine børn er flyttet fra ægtefællen og kommer og indleverer en flytteblanket – må have adgang til at se, hvilke typer af sager, der verserer i kommunen vedrørende borgeren eller dennes børn, f.eks. sager om boligstøtte, børnebidrag, delvis friplads i institution og lign.

De må dog ikke have adgang til de mest følsomme sager, f.eks. sager om undersøgelser af mulig vanrøgt eller misbrug af børn, sager om frivillig anbringelse uden for hjemmet, sager om en hel families døgnophold på en familieinstitution, sager om undersøgelser af muligt socialt bedrageri eller sager oprettet i forbindelse med SSP-samarbejdet.

Adgang til andre myndigheders oplysninger

Nogle gange indgår der oplysninger i kommunernes systemer, der hører til andre myndigheder. Det er især relevant, hvis kommunen fungerer som sekretariat for en anden myndighed.

Børn og unge-udvalgets sager

Eksempelvis er Børn og unge-udvalget, som tager stilling i særlige sager om udsatte børn og unge som f.eks. tvangsmæssige anbringelser uden for hjemmet, en selvstændig myndighed og ikke en del af kommunen. Børn og unge-udvalget får sekretariatsbistand af kommunale medarbejdere.

Kun de medarbejdere, der arbejder i børn og unge-udvalgets sekretariat, må have adgang til oplysninger om børn og unge-udvalgssager. Herunder oplysninger om, at sagerne overhovedet findes.

Adgangen til børn og unge-udvalgets sager skal derfor teknisk kunne begrænses, så kun de medarbejdere, der yder sekretariatsbistand, kan få adgang.

Andre sager, der hører til andre myndigheder

Kommunale medarbejdere yder også sekretariatsbistand i forhold til andre selvstændige myndigheder, som træffer afgørelser m.v. over for kommunens borgere. Det gælder f.eks. vielsesmyndigheden (borgmesteren), folkeoplysningsudvalg, bevillingsnævn, huslejenævn og hegnsyn. Adgangen til de sager, der hører under disse myndigheder, skal også teknisk kunne begrænses, så kun de relevante medarbejdere får adgang.

Se i øvrigt afsnit 3.4.

Afklaring af det reelle behov

I forbindelse med rettighedsopsætning af eksisterende it-systemer eller en eventuel udarbejdelse af kravspecifikationer til ny it-understøttelse skal det afklares, om systemet skal bruges til flere forskellige opgaver. Hvis systemet skal bruges til flere forskellige opgaver, skal det afklares, hvordan adgangen til oplysningerne skal kunne opdeles.

Det anbefales, at medarbejdernes behov for adgang til oplysninger afklares i et samarbejde med medarbejdere med indsigt i, hvilke sagstyper / oplysninger der er behov for adgang til, for at medarbejderne kan løse de opgaver, der er henlagt til borgerservicecenteret.

Gælder hele kommunen

Kravet om differentieret adgang gælder for it-systemer, der bruges i alle dele af den kommunale forvaltning – ikke kun for borgerservicecentrene. Men kravet kan være særligt relevant for it-systemer, der bruges af medarbejdere i borgerservicecentre, fordi der netop her ofte kan være behov for en bredere adgang til enkelte oplysninger (navnlig hvor der gives en mere overordnet vejledning af borgere, der befinder sig i en bestemt livssituation).

1.2. Generering af log, kontrol og adgang til loggen

Hvornår logning?

Mange former for elektronisk databehandling i it-systemer skal anmeldes til Datatilsynet inden iværksættelse. Det gælder især databehandling, der omfatter fortrolige eller følsomme oplysninger[3].

Som udgangspunkt skal alle anvendelser af personoplysninger, som er omfattet af anmeldelsespligten, logges, dvs. maskinelt registreres[4].

[3] Jf. kapitel 12 i persondataloven og reglerne i anmeldelsesbekendtgørelsen (bekendtgørelse nr. 529 af 25. september 2000 om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for den offentlige forvaltning)
http://www.datatilsynet.dk/include/show.article.asp?art_id=496&sub_url=/lovgivning/indhold.asp

Hvorfor logning?

Loggen fungerer som et teknisk revisionsspor, hvis der er mistanke om misbrug af oplysninger, eksempelvis ved at medarbejdere kigger i oplysninger, som ikke er relevante for deres opgaveløsning.

Den skal derfor kunne rekvireres til enhver tid, og indholdet (f.eks. koder) skal kunne forstås af it-medarbejderne / sikkerhedsmedarbejderne.

Særlige krav til borgerservicecentre

Logningskravet gælder i forhold til it-systemer i alle dele af kommunen, men det spiller en særlig rolle i forhold til borgerservicecentrene.

Datatilsynet stiller nemlig krav om, at borgerservicecentrene styrker datasikkerheden i borgerservicecentrene.

Hvorfor særlige krav?

De større krav skyldes, at medarbejderne i borgerservicecentrene ofte på grund af deres brede opgavesammensætning har adgang til flere it-systemer med personoplysninger, end kommunale medarbejdere, som arbejder med mere afgrænsede opgaver.

Datatilsynets krav

For at styrke datasikkerheden i borgerservicecentrene stiller Datatilsynet krav om, at kommunerne foretager ***stikprøver*** af loggen fra anmeldelsespligtige systemer (normalt systemer med følsomme eller fortrolige oplysninger).

Der kan eventuelt også være andre metoder til at styrke datasikkerheden, som kan træde i stedet for stikprøvekontrollen. Datatilsynet vil være indstillet på at lade den manuelle stikprøvekontrol erstatte af en ***automatiseret overvågning***, der bl.a. afdækker uhensigtsmæssige eller usædvanlige søgemønstre og dermed er bedre egnet end stikprøvekontrol til at afsløre misbrug. Kommunen kan altid kontakte Datatilsynet og drøfte sådanne alternative løsninger.

Administrationen af kontrolordningerne er nærmere beskrevet i afsnit 5.

Det vil være naturligt, at det er kommunalbestyrelsen eller kommunens ledelse, som træffer afgørelse om, på hvilken måde kommunen vil styrke datasikkerheden i borgerservicecenteret.

Stikprøvekontrol

Stikprøvekontrol stiller ikke yderligere krav til it-systemerne end dem, der allerede gælder. Det kan dog overvejes – hvis det er teknisk og praktisk muligt – at orientere medarbejderne på systemets åbningsbillede om, at der foretages jævnlige stikprøvekontroller af de opslag, som medarbejderen foretager i systemet. Om administrationen af stikprøvekontrolordninger; se afsnit 5.2.

---

[4] Jf. § 19, stk. 1, i sikkerhedsbekendtgørelsen. Efter § 19, stk. 2, gælder dette ikke personoplysninger, som indgår i tekstbehandlingsdokumenter og lignende, der ikke foreligger i endelig form, eller dokumenter i endelig form, der slettes inden 30 dage.

Automatisk overvågning

Derimod stiller automatiseret overvågning af loggen krav om en særlig teknisk løsning, som kan opdage søgemønstre efter særlige kriterier. Det kan f.eks. være opslag på oplysninger om kendte personer eller borgere i andre kommuner, opslag uden for normal åbningstid, opslag på følsomme sager, der er afsluttet, opslag i samme system på oplysninger om mange forskellige personer inden for et kort tidsrum eller lign.

Det forudsætter, at der opstilles nogle særlige kriterier for, hvilke opslag den tekniske løsning skal kunne udpege som uhensigtsmæssige eller usædvanlige.

Det anbefales, at kriterierne opstilles i samarbejde med medarbejdere, der kender borgerservicecenterets opgaver og arbejdsgange.

Borgernes adgang til loggen

Som et supplement til stikprøvekontrol af loggen eller automatiseret overvågning kan kommunen desuden vælge at give borgerne adgang til log-oplysninger. En sådan adgang vil især være værdifuld for borgerne.

Hvis en sådan løsning etableres, skal angivelsen af, hvem der har indhentet oplysninger om en borger, ske på et niveau, der er relevant og tilstrækkeligt præcist til, at løsningen kan tjene sig formål.

Findes ikke systemer i dag

Der findes ikke på nuværende tidspunkt nogle kommunale systemer, som kan vise borgeren en overordnet log i et digitalt selvbetjeningssystem.

At etablere en ordning, hvor borgerne gives adgang til log-oplysninger, kræver overvejelser omkring både de persondataretlige regler og nogle mere generelle forvaltningsjuridiske og administrative problemstillinger. Datatilsynet opfordrer kommuner, der overvejer at etablere borgeradgang til log-oplysninger, til at kontakte tilsynet for at drøfte udformning, sikkerhedsniveau m.v. KL kan kontaktes vedrørende øvrige juridiske og administrative overvejelser.

1.3. Skærmlås og automatisk log off

Arbejdsstationer i borgerservicecentrene skal beskyttes med en automatik, som forhindrer uvedkommende i at få adgang til personoplysninger. Det skyldes, at der i borgerservicecentrene ofte er mange personer til stede i de lokaler, hvor medarbejderne slår op i mange forskellige it-systemer med personoplysninger. Automatikken kan bestå i en skærmlås og / eller automatisk log off.

Automatikken er en sikkerhedsforanstaltning, som har til formål at afbryde adgangen til programmer og data i de tilfælde, hvor medarbejderen har glemt manuelt at afbryde adgangen, før han eller hun

forlader sin skærm.

Såvel skærmlås som automatisk log off skal sættes op på en sådan måde, at funktionen udføres efter en vis kortere periode uden aktivitet. Det kan f.eks. være 15 – 20 min.

Funktionen skal opsættes i overensstemmelse med god sikkerhedspolitik, det vil sige, at medarbejderne ikke selv skal kunne ændre intervallet, før funktionen aktiveres, eller fravælge funktionen.

Når brugeren skal aktivere en skærm, som automatisk er blevet låst, eller foretage en fornyet log on til et system, som har foretaget automatisk log off, skal der ske fornyet indtastning af password.

Selvom et system ikke indeholder personoplysninger, kan det også i nogle tilfælde være hensigtsmæssigt at bruge skærmlås og / eller automatisk log off, hvis systemet indeholder fortrolige oplysninger om virksomheder, foreninger og lign.

Gælder hele kommunen?

Kravene om skærmlås og / eller automatisk log off er sikkerhedsforanstaltninger, som også bør være implementeret andre steder i kommunen, hvor det skønnes nødvendigt for at sikre, at kun autoriserede brugere kan få adgang til de personoplysninger og anvendelser, som de er autoriserede til.

1.4. Digital kommunikation med borgerne

Kommunikation via e-post og digitale selvbetjeningsløsninger

Når borgerservicecenteret kommunikerer via internettet med borgerne om personoplysninger skal kommunikationen være sikret mod, at oplysningerne kommer til uvedkommendes kendskab[5]. Dette gælder både e-postkommunikation, og når borgeren f.eks. indsender oplysninger via en selvbetjeningsløsning på kommunens hjemmeside.

Kommunen skal ved brug af digital signatur og eventuelt andre løsninger sikre sig, at oplysningerne stammer fra borgeren selv.

Krav til e-postkommunikation

Skal borgerservicecenteret kunne sende følsomme eller fortrolige personoplysninger i en e-post til borgeren over internettet, skal e-posten kunne sendes som sikker e-post, dvs. signeret og krypteret.

Krav til selvbetjeningsløsninger

Selvbetjeningsløsninger hvor borgeren skal oplyse følsomme eller fortrolige oplysninger, f.eks. oplysninger om cpr-nummer, helbred eller økonomi, bør indrettes sådan, at borgeren for at kunne indsende oplysningerne skal have identificeret sig via digital signatur.

Er en given selvbetjeningsløsning indrettet sådan, at borgerens oplysninger bliver sendt over internettet for at komme frem til kommunen,

[5] Jf. § 41, stk. 3, i persondataloven

skal fremsendelsen ske via en sikker forbindelse.

Hvis en kommune etablerer selvbetjeningsløsninger på internettet eller lign., yder Datatilsynet vejledning om, hvordan sikkerheden skal være for at beskytte personoplysningerne.

Gælder hele kommunen

Kravene om sikker netkommunikation gælder for hele kommunen. Kravene til sikker e-postkommunikation kan imidlertid være særligt relevante for borgerservicecentrene, der har megen borgerkontakt, idet borgerkontakten for mange borgerservicecentres vedkommende også sker via e-post. Borgerservicecentrene vil også ofte have særlige funktioner i forhold til digitale selvbetjeningsløsninger, f.eks. i form af sagsbehandling i forlængelse af borgernes brug af løsningerne.

1.5. Andre krav i forbindelse med indretningen af it-systemerne

Alle kommunale it-systemer – herunder borgerservicecenterets it-systemer – skal også kunne leve op til andre persondataretlige krav (ligesom de skal kunne leve op til f.eks. forvaltningsretlige og arkivmæssige krav).

It-systemerne skal f.eks. tage højde for tildeling af særskilte rettigheder til inddatering og sletning, datakvalitet / ajourføring, sletterutiner, indsigtsret / aktindsigt, oplysningspligt, berigtigelse og tilbagekaldelse af samtykke samt registrering af (og blokering ved) uautoriserede adgangsforsøg og sikkerhed ved brug af eksterne kommunikationsforbindelser. Se mere i sikkerhedsbekendtgørelsen.

2. Hvordan skal edb-udstyr og lign. placeres?

Sikkerhedsmedarbejderne / it-medarbejderne skal nøje overveje, hvor og hvordan borgerservicecenterets edb-udstyr anbringes. De skal også overveje, hvor og hvordan inddatamateriale og uddatamateriale kan opbevares, når det ikke bruges af medarbejderne.

Hvorfor særlig håndtering?

Personoplysninger må ikke komme til uvedkommendes kendskab. Borgere og andre uden for kommunens administration er normalt uvedkommende. Det er meget uheldigt, hvis en borger under et besøg i borgerservicecenteret kan se fortrolige eller følsomme oplysninger om andre borgere.

Edb-udstyr

Computerskærme skal stå sådan, at borgerne ikke kan se personoplysninger om andre borgere på skærmene. Printere, kopimaskiner, skannere, multimaskiner og lign. skal anbringes sådan, at borgerne ikke har adgang til udskrifter m.v. De må f.eks. normalt ikke stå ud til et areal, hvor borgerne har adgang. Alternativt kan kommunen evt. bruge udstyr, som lagrer udskrifterne i maskinen, indtil medarbejderne står klar ved apparatet og indtaster en kode.

Telefaxmaskiner skal også anbringes sådan, at borgerne ikke har adgang til at se indkomne eller afsendte telefaxer. Her kan kommunen evt. på samme måde bruge udstyr, der lagrer telefaxerne, indtil en medarbejder indtaster en kode og udskriver dem eller sender dem videre til den relevante medarbejders e-postadresse.

Døren til serverrum bør altid være aflåst, hvilket især er vigtigt, hvis rummet ligger i tilknytning til publikumsarealet.

Ind- og uddata-materiale

Inddatamateriale med fortrolige eller følsomme oplysninger skal opbevares aflåst, når det ikke bruges. Sikkerhedsmedarbejderne må med andre ord sørge for, at der er et lokale, skab eller lign., som medarbejderne kan låse den type af materiale ind i.

Brug af uddatamateriale – f.eks. udskrifter – med personoplysninger skal også leve op til særlige regler i sikkerhedsbekendtgørelsen[6], herunder regler om tilintetgørelse og om hvilke medarbejdere, der må have adgang til uddatamaterialet.

[6] Jf. § 13 i sikkerhedsbekendtgørelsen

Med hensyn til ind- og uddatamateriale skal der fastsættes formelle retningslinier for, hvordan det skal håndteres, når det ikke bruges. Retningslinierne skal fremgå af kommunens uddybende sikkerhedsregler[7]. Kommunen bør også overveje, om der er behov for at opstille en papircontainer til papirer med fortrolige eller følsomme oplysninger, som skal smides ud, f.eks. brevudkast i sociale sager og lign. En sådan container bør være aflåst eller placeret i et område, der er aflåst uden for arbejdstiden, og hvor borgerne ikke har adgang i åbningstiden. Hvis papirkurve bruges til fortroligt materiale, skal de også anbringes, så borgerne ikke har mulighed for at få fat i indholdet.

Hvad er inddata- og uddatamateriale?

Inddatamateriale: Grundmateriale (papirbaseret eller elektronisk), hvorfra der hentes personoplysninger til videre elektronisk databehandling, f.eks. ansøgningsskemaer, der skal tastes ind eller e-post fra borgere, der skal journaliseres på en elektronisk sag. (Dog ikke papirer fra papirbaserede sager.)

Uddatamateriale: Resultatet af en elektronisk databehandling, som foreligger i papirbaseret eller elektronisk form, f.eks. udskrifter af breve, skærmprints, lister osv., som indeholder personoplysninger. (Dog ikke papirer, der indgår i papirbaserede sager.)

Uanset reglerne i sikkerhedsbekendtgørelsen ikke gælder for papirbaserede sager, skal de dog også opbevares med omtanke.

Gælder hele kommunen

Kravene gælder i forhold til edb-udstyr, inddata- og uddatamateriale, der bruges i alle dele af kommunen. Men kravene kan være særlig relevante for borgerservicecentrene, fordi borgerne netop her ofte er meget tæt på medarbejderne, edb-udstyret og ind- og uddatamaterialet.

[7] Jf. § 5 i sikkerhedsbekendtgørelsen

3. Hvem må have adgang til it-systemerne?

3.1. Autorisationsordninger

At meddele en medarbejder autorisation består normalt i, at sikkerhedsmedarbejderne / it-medarbejderne tildeler medarbejderen en brugeridentifikation og et personligt password. Autorisationen giver herefter adgang til bestemte it-systemer, eventuelt bestemte dele af it-systemerne.

Der skal fastlægges en formel autorisationsprocedure og –arbejdsgang[8]. Den skal indgå i kommunens uddybende sikkerhedsregler.

Ikke fælleskoder

Mange former for elektronisk databehandling i it-systemer skal anmeldes til Datatilsynet inden iværksættelse. Det gælder især databehandling, der omfatter fortrolige eller følsomme oplysninger[9].

Til anmeldelsespligtige it-systemer må der ikke tildeles fælleskoder, dvs. koder, der bruges af flere medarbejdere. Det gælder uanset, at flere medarbejdere har behov for adgang til samme systemer.

Selvom der er tale om et system, som der ikke er anmeldelsespligtigt, anbefales det at undgå fælleskoder.

Ikke "Fælles Pinkode"

Medarbejderne bør heller ikke anvende deres private "Fælles Pinkode" som adgangskode til kommunens it-systemer i arbejdsmæssig sammenhæng[10].

Hvorfor individuelle/ særskilte koder?

En log kan ikke bruges til at opklare et eventuelt misbrug, hvis flere medarbejdere bruger den samme kode. Se nærmere i afsnit 1.3. Derfor er det nødvendigt at tildele individuelle koder til medarbejderne.

Men fælleskoder er heller ikke anbefalelsesværdige i forhold til systemer, som ikke skal logges. Hvis f.eks. 10 personer har den samme kode, og én skifter arbejdsområde og derfor ikke længere må have adgang, skal de øvrige 9 kolleger have en ny kode.

---

[8] Jf. § 5, stk. 1, i sikkerhedsbekendtgørelsen

[9] Jf. kapitel 12 i persondataloven og reglerne i anmeldelsesbekendtgørelsen (bekendtgørelse nr. 529 af 25. september 2000 om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for den offentlige forvaltning)
http://www.datatilsynet.dk/include/show.article.asp?art_id=496&sub_url=/lovgivning/indhold.asp

[10] Datatilsynets udtalelse af 26. september 2005
http://www.datatilsynet.dk/attachments/2005630122154/Brev%20af%202005-09-26%20til%20M%20Kommune.pdf

3.2. Autorisation kun til de nødvendige it-systemer / sager / oplysninger

Adgang til it-systemer

Medarbejdere må kun autoriseres til at have adgang til it-systemer, som de har brug for i deres arbejde. Adgangen skal være sagligt begrundet.

En medarbejder må ikke autoriseres til at have adgang til alle de offentlige it-systemer, som medarbejderen teoretisk kan tænkes at skulle bruge oplysninger fra. Det må afklares, om opslag i it-systemerne vil være en *del af medarbejderens almindelige opgaver*. Der må ikke gives adgang til it-systemer, som medarbejderen kun i usædvanlige situationer vil få brug for.

Eksempelboks 3

Et borgerservicecenter har en gruppe medarbejdere, der arbejder med folkeregistrering. Der er 2 – 3 folkeregistermedarbejdere til stede hver dag. Det kan teoretisk forekomme, at alle medarbejdere i folkeregistersektionen en dag er fraværende på grund af uforudsigelige sammentræf (sygdom eller lign.). En kollega i f.eks. boligstøttesektionen må ikke være autoriseret til CPR for det tilfælde, at den teoretiske situation skulle opstå. Hvis bemandingen derimod er sådan, at en kollega som en normal opgave vikarierer i folkeregistersektionen ved fravær, må kollegaen gerne autoriseres.

Adgang til sager / oplysninger

Hvis et bestemt system bruges til flere forskellige opgaver, skal medarbejderens adgang begrænses til de oplysninger i systemet, som vedrører de opgaver, han eller hun beskæftiger sig med.

Det er navnlig relevant i forhold til it-systemer, som bruges til mange forskellige sagstyper og dermed opgaver, f.eks. ESDH-systemer, tekstbehandlingssystemer, e-postsystemer og andre it-systemer, som bruges på tværs af forskellige kommunale opgaver.

Autorisationen kan f.eks. begrænses til de oplysninger, der vedrører de *sagstyper*, som medarbejderen arbejder med.

Autorisationen kan også begrænses til oplysninger på et bestemt *niveau*. Det kan f.eks. eventuelt være sagligt velbegrundet, at medarbejderen kan se, at borgeren har en bestemt sag verserende i kommunen, hvorimod det måske ikke er sagligt velbegrundet, at medarbejderen har adgang til de underliggende oplysninger / dokumenter, der hører til sagen.

Eksistensen af visse sager eller sagstyper er i sig selv en fortrolig oplysning, og skal derfor hemmeligholdes. Disse må således ikke kunne ses af andre end dem, der beskæftiger sig med den konkrete type af sager. De må f.eks. ikke fremgå af almindelige sagsoversigter, som er tilgængelige for medarbejdere, hvis opgave alene er at vejlede borgere, der befinder sig i en almindeligt forekommende livssituation.

Eksempelboks 4

Kun medarbejdere, der arbejder med sager om f.eks. undersøgelser af mulig vanrøgt eller misbrug af børn, sager om frivillig anbringelse uden for hjemmet, sager om en hel families døgnophold på en familieinstitution, sager om undersøgelser af muligt socialt bedrageri eller sager oprettet i forbindelse med SSP-samarbejdet, må kunne se, at kommunen behandler eller har behandlet en sådan sag.

Inddatering og sletning

I forhold til it-systemer, der er anmeldelsespligtige, skal der ved autorisationen også tages stilling til, om medarbejderne må søge på, inddatere eller slette oplysninger.[11]

Inddragelse af ledelsen

IT-medarbejderne / sikkerhedsmedarbejderne må afklare med de relevante ledere i kommunen, hvilke rettigheder til at søge, inddatere eller slette medarbejdere eller grupper af medarbejdere skal have.

Hvorfor differentieret adgang?

Ved at opdele adgangen til de relevante sager eller oplysninger kan kommunen sikre, at oplysninger om borgerne (heriblandt fortrolige eller følsomme oplysninger) ikke kan ses af medarbejdere, som ikke har brug for oplysningerne.

Gælder hele kommunen

Kravet om differentieret adgang gælder for alle it-systemer, der bruges i hele den kommunale forvaltning – ikke kun for borgerservicecentrenes it-systemer. Men kravet kan være særligt relevant for it-systemer, der bruges af medarbejdere i borgerservicecentre, fordi der netop her ofte kan være behov for en bredere adgang til enkelte oplysninger (navnlig hvor der gives en mere overordnet vejledning af borgere, der befinder sig i en bestemt livssituation).

[11] Jf. § 16 i sikkerhedsbekendtgørelsen

3.3. Inddragelse af autorisationer

For medarbejdere, som ikke længere har behov for de autorisationer, som de har fået, skal autorisationerne *inddrages*. Det gælder f.eks. medarbejdere, som får et andet arbejdsområde. Endvidere skal kommunen i forhold til anmeldelsespligtige it-systemer mindst en gang hver halve år sikre sig, at de autoriserede personer fortsat opfylder autorisationsbetingelserne[12].

Gælder hele kommunen

Reglerne om inddragelse af autorisationer gælder for hele kommunen. Men behovet for inddragelse af autorisationer kan være særlig relevant i borgerservicecentre, hvis medarbejderne ofte skifter arbejdsopgaver internt eller f.eks. i forbindelse med indstationeringer fra fagforvaltningerne.

3.4. Adgang til andre myndigheders it-systemer

Samarbejde med den anden myndighed

Hvis medarbejderne, f.eks. i borgerservicecenteret, har behov for adgang til en anden myndigheds elektroniske system, må den anden myndighed tage stilling til, om videregivelsesbetingelserne[13] i lovgivningen er opfyldt, og om systemet og behovet for oplysningerne er af en sådan karakter, at borgerservicecentermedarbejderne kan få adgang.

Hvis kommunens medarbejdere inddaterer eller i øvrigt behandler oplysninger på vegne af den anden (dataansvarlige) myndighed, skal der normalt indgås en skriftlig databehandleraftale[14].

Datasikkerheden skal varetages i samarbejde med den dataansvarlige myndighed.

På skatteområdet er der udgivet en vejledning, hvor samarbejdet mellem kommunerne og staten for så vidt angår datasikkerhed er beskrevet[15].

En del af kommunens systemer

I nogle tilfælde fungerer kommunen som sekretariat for en anden myndighed. F.eks. sekretariatsbetjenes kommunens børn og ungeudvalg (der er en selvstændig myndighed) af kommunale medarbejdere. Se andre eksempler i afsnit 1.1. Disse myndigheder vil ofte ikke have et selvstændigt it-system. Tværtimod vil sekretariatet – dvs. de kommunale medarbejdere – som regel bruge kommunens egne sy-

---

[12] Jf. § 17 i sikkerhedsbekendtgørelsen

[13] F.eks. behandlingsreglerne i persondataloven, § 3, stk. 1 eller 6, i borgerservicecenterloven eller bestemmelser i særlovgivningen

[14] Jf. § 42, stk. 2, i persondataloven

[15] Vejledning om kommuners borgerbetjening på skatteområdet
http://www.skat.dk/SKAT.aspx?oID=351152&vID=201112

stemer.

Uanset sagerne / oplysningerne indgår i kommunens egne it-systemer, hører de stadig under den anden myndighed.

Hvis der er et ønske om at give adgang til sagerne / oplysningerne til kommunale medarbejdere, der ikke sekretariatsbetjener myndigheden, svarer det til at give adgang til en anden myndigheds systemer. Det gælder også adgang til oplysninger om, at der overhovedet eksisterer en sag. I så fald skal myndigheden tage stilling til, i hvilket omfang videregivelsesbetingelserne[16] er opfyldt, og om der kan etableres en adgang, der er begrænset til de sager / oplysninger i it-systemet, som må videregives.

[16] F.eks. behandlingsreglerne i persondataloven eller bestemmelser i særlovgivningen

4. Hvordan skal medarbejderne instrueres om datasikkerhed?

Kommunen har pligt til at give de medarbejdere, som behandler personoplysninger, den fornødne instruktion. Medarbejderne skal orienteres om kommunens uddybende sikkerhedsregler[17] og eventuelt andet materiale om datasikkerhed. Det er forudsætningen for, at medarbejderne kan følge de sikkerhedsregler, der er relevante for dem.

De særlige træk ved borgerservicecentrene betyder, at kommunen i forhold til medarbejdere i borgerservicecentre skal have *særligt* fokus på uddannelse og vejledning i datasikkerhed.

	Medarbejderne skal især instrueres i:
Aldrig usaglige, herunder private, opslag	Medarbejderne må aldrig bruge deres adgang til et elektronisk system til usaglige formål. Private formål betragtes altid som usaglige, uanset hvilke private formål det drejer sig om. Det gælder bl.a., hvis medarbejderne ønsker at få aktindsigt i en sag efter offentlighedsloven. Kommunen kan dog have særlige retningslinier for, hvorvidt medarbejderne må slå op på oplysninger om dem selv med henblik på indsigt efter persondataloven eller partsaktindsigt efter forvaltningsloven.
	Eksempelboks 5 En medarbejder skal indkalde til fest for sine gamle klassekammerater. Hun slår op i kommunens p-datasystem for at finde deres nye adresser. Opslaget er ikke berettiget.
Ikke genbrug til uforenelige opgaver	Oplysninger, der er indsamlet og registreret til brug for en bestemt opgave, må ikke efterfølgende genbruges til en anden opgave, hvis det er uforeneligt med den oprindelige opgave[18]. Brug til formål, der ellers ville være uforenelige, kan kun ske, hvis borgeren har givet samtykke.

[17] Jf. § 6 i sikkerhedsbekendtgørelsen

[18] Jf. § 5, stk. 2, i persondataloven (finalité-princippet)

	Eksempelboks 6 X Kommune har slået en ledig stilling i borgerservicecenteret op. Borgerservicecenteret skal have en person til samtale, som eventuelt skal ansættes. En af de medarbejdere, der skal være med ved samtalen, mener at kunne huske, at ansøgeren er den borger, der tidligere har skrevet nogle vrede breve til kommunen i en boligstøttesag. Hun tænker, at det er vigtigt, at deres nye medarbejder har en god tone over for borgerne. Hun slår derfor op i boligstøttesystemet for at se, om ansøgeren er den borger, der tidligere har haft en boligstøttesag i kommunen. Opslaget er ikke berettiget. Det er ikke foreneligt med det oprindelige formål (at behandle boligstøttesager), at oplysningerne bruges i forbindelse med en ansættelsessag.
	Eksempelboks 7 X Kommune har modtaget en flyttemeddelelse om, at en familie med et skolebarn flytter til en bestemt adresse i byen. Flyttemeddelelsen indtastes i CPR. Oplysninger fra flyttemeddelelsen bruges i forbindelse med den relevante skoles udsendelse af materiale om opskrivning til skolen. Opslaget i CPR er berettiget.
Huske at logge ud	Medarbejderne må ikke gå i længere tid fra en pc uden at logge sig selv ud. Det gælder også, selvom pladsen overtages af en kollega, som har de samme arbejdsopgaver.
	Eksempelboks 8 Medarbejderen har siddet ude ved skranken om formiddagen og betjent forskellige borgere. Om eftermiddagen arbejder medarbejderen to timer i et ”stille-rum” for at behandle nogle lidt mere komplicerede folkeregistersager, mens en kollega sidder i skranken. Den sidste time inden borgerservicecenteret lukker, skal medarbejderen sidde i skranken igen. Medarbejderen skal logge sig ud i de to timer, hvor vedkommende ikke sidder i skranken.
Huske fortroligheds-hensynet	Medarbejderne skal være særligt opmærksomme på, at skærme og papirer ikke vender eller ligger sådan, at borgere kan komme til at se indholdet.

Kende regler om e-post	Medarbejderne skal kende reglerne for elektronisk kommunikation med borgere, herunder digital signatur. Medarbejderne må f.eks. ikke sende e-post med fortrolige personoplysninger uden at signere og kryptere e-posten. Se også afsnit 1.4.

Hvordan kan eller skal instruktionen gives?

Instruktion kan gives på flere forskellige måder.

Alle kommuner skal have uddybende sikkerhedsregler, og derudover kan de have særlige instrukser og informationsmateriale til medarbejderne. Det er ofte en god idé at lægge kommunens uddybende sikkerhedsregler og lign. materiale (dog ikke bilag, som af sikkerhedsmæssige årsager skal hemmeligholdes) på et intranet.

Derudover kan det være hensigtsmæssigt at lave en folder med de afsnit fra de uddybende sikkerhedsregler, der er særligt relevante for medarbejderne i borgerservicecenteret, eller sikkerhedsvejledninger i forhold til bestemte situationer, f.eks. forsendelse af e-post til borgere.

Materialet kan også uddeles som en del af en "velkomstpakke" til nye medarbejdere i borgerservicecenteret, hvori der også ligger andet materiale, som medarbejderen bør kende.

Datatilsynets krav

Datatilsynet forudsætter, at medarbejderne i borgerservicecentrene får særlig instruktion i datasikkerhed.

Forslag til særlig instruktion

Dette kan f.eks. ske ved:

1) Et kort, f.eks. halvdags, undervisningsforløb, som alle medarbejdere skal gennemføre, inden de starter i borgerservicecenteret. Det kan f.eks. ske som sidemandsoplæring eller ved at deltage i et relevant eksternt eller internt kursus. Et eventuelt internt undervisningsforløb kan f.eks. tage udgangspunkt i kommunens uddybende sikkerhedsregler og øvrige datasikkerhedsinstrukser

2) Et "datasikkerhedskørekort", som alle medarbejdere skal tage, inden de starter i borgerservicecenteret. Det kan f.eks. være en test med et antal spørgsmål, som forudsætter den fornødne viden om kommunens uddybende sikkerhedsregler og øvrige datasikkerhedsinstrukser, før medarbejderen vil kunne besvare den korrekt.

Kommunen skal sikre sig, at det står helt klart for medarbejderne, hvilke regler, procedurer osv. de skal overholde, og at kommunen lægger vægt på overholdelsen. Det kan f.eks. ske gennem den kvalificerede instruktion, der er nævnt ovenfor. Kommunen kan også give egentlige tjenestebefalinger. Tydelig instruktion og / eller tjenestebefalinger har betydning for muligheden for, at medarbejderen kan ifalde disciplinære sanktioner for eventuelle overtrædelser.

5. Valg og administration af kontrolordninger

5.1. Forskellige kontrolordninger

Datatilsynet stiller krav om, at kommunerne styrker datasikkerheden i borgerservicecentrene[19], og deri ligger bl.a., at adgangskontrol og autorisationer skal suppleres af passende kontrolordninger.

Det vil være naturligt, at det er kommunalbestyrelsen eller kommunens ledelse, som træffer afgørelse om, på hvilken måde kommunen vil styrke datasikkerheden i borgerservicecenteret.

Kommunens beslutninger om datasikkerhed skal fremgå af kommunens uddybende sikkerhedsregler.

Manuel eller automatisk kontrol af loggen

Datatilsynet henstiller bl.a., at kommunerne foretager stikprøver af loggen fra anmeldelsespligtige systemer (normalt systemer med følsomme eller fortrolige oplysninger), eller eventuelt alternativt indfører automatiseret overvågning af uhensigtsmæssige eller usædvanlige søgemønstre.

Formålet med en stikprøvekontrol eller automatiseret overvågning af loggen er dels at afsløre eventuelt misbrug, dels at forebygge misbrug. Stikprøvekontrollerne forudsætter ikke i sig selv nogen særlig indretning af kommunens it-systemer, idet der i forvejen stilles krav om, at der sker logning. Det gør automatiseret overvågning imidlertid.

Der skal fastlægges rutiner i forbindelse med stikprøverne eller eventuel automatiseret overvågning.

Se mere om stikprøver i afsnit 5.2. og om overvågning i afsnit 5.3.

Borgerens adgang til log-oplysninger

Derudover kan kommunerne vælge at give borgerne adgang til en log via en elektronisk selvbetjeningsløsning. Det er ikke et krav. Hvis en kommune ønsker, at en sådan ordning erstatter de to første, skal kommunen forinden kontakte Datatilsynet.

Borgerens adgang til log-oplysninger forudsætter, at it-systemerne indrettes sådan, at de kan generere en log. Der findes ikke på nuværende tidspunkt nogle kommunale systemer, som kan generere en log i et digitalt selvbetjeningssystem.

Hvis kommunen ønsker at få udviklet et system, som kan give borgerne adgang til en overordnet log, er der nogle forhold, kommunen skal være opmærksom på. Se nærmere i afsnit 1.2.

---

[19] Jf. Datarådets udtalelse af 7. januar 2005 om borgerservicecenterloven. Gengivet i Datatilsynets årsberetning for 2004 http://www.datatilsynet.dk/publikationer/aarsrapport04/kap02.htm

Andre kontrolordninger

Der kan eventuelt også være andre metoder til at styrke datasikkerheden, herunder i form af kontrolordninger. Kommunen kan altid kontakte Datatilsynet og drøfte sådanne alternative løsninger.

5.2. Stikprøve af loggen

Stikprøver af loggen skal foretages på kommunens eget initiativ.

Stikprøverne bør tages med jævne mellemrum for at opnå den præventive effekt, som er en af de væsentligste årsager til stikprøverne.

Stikprøverne bør tages med vilkårlige intervaller, så ingen vil kunne forudsige, hvornår de foretages, og indrette sig efter det. Intervallerne kan eventuelt skrives i et fortroligt bilag til kommunens uddybende sikkerhedsregler.

Det vil være naturligt, at det er kommunens ledelse, der beslutter, hvordan kontrollen skal foretages, herunder hvilke personer der skal involveres i kontrollen. Proceduren kan eventuelt skrives ind i kommunens uddybende sikkerhedsregler.

Stikprøverne bør dække en periode, som ligger tæt på det tidspunkt, hvor resultatet af stikprøverne præsenteres for den medarbejder, som har foretaget opslagene. Det vil give medarbejderen bedst mulighed for at huske årsagen til opslagene.

Eksempelboks 9:

I X Kommunes uddybende sikkerhedsregler står der:

> **Stikprøver af loggen**
> Stikprøverne foretages af de opslag, som borgerservicecentermedarbejderne foretager i de logningspligtige it-systemer. Stikprøverne falder med forskellige intervaller, f.eks. 1 måned, 2½ måned, 5 måneder, 3 måneder osv., dog højst 6 måneder. Datoerne fremgår af et bilag, som kun sikkerhedsmedarbejderne har adgang til.
>
> En stikprøve omfatter 5 – 6 opslag foretaget 1 – 3 dage før, medarbejderen anmodes om at redegøre for årsagen til opslagene.
>
> Stikprøverne udskrives og forelægges de medarbejdere, der har foretaget opslagene. De skriver på udskriften, hvad årsagen til opslagene var (evt. journalnumre på de sager, som opslagene vedrørte). Stikprøverne med medarbejderens noteringer lægges til den chef, som har den største indsigt i vedkommendes arbejde. Giver det chefen anledning til spørgsmål, taler chefen med medarbejderen / sikkerhedsmedarbejderen. Giver det ikke anledning til spørgsmål, betragtes kontrollen som gennemført med tilfredsstillende resultat.

> Hver 2. måned udsendes en meddelelse på intranettet om, at opslag i de fleste af kommunens it-systemer logges, at opslagene til enhver tid kan blive kontrolleret, og at de opslag, som borgerservicecenter-medarbejderne foretager, kontrolleres jævnligt ved stikprøver. I de af kommunens it-systemer, hvor det er muligt at tilpasse åbningsbilledet, står samme besked.

Datatilsynets krav

Datatilsynet henstiller, at kommunerne foretager stikprøvekontrol i et omfang, der svarer til eksemplet i eksempelboks 9.

5.3. Automatiseret overvågning

Automatiseret overvågning er en teknisk løsning, som automatisk finder og giver sikkerhedsmedarbejderne meddelelse om uhensigtsmæssige eller usædvanlige søgemønstre.

Det forudsætter, at der opstilles nogle særlige kriterier for, hvornår søgemønstre er uhensigtsmæssige eller usædvanlige.

Det kan f.eks. være opslag på oplysninger om kendte personer, opslag uden for normal åbningstid, opslag på følsomme sager, der er afsluttet, opslag i samme system på oplysninger om mange forskellige personer inden for et kort tidsrum eller lign. Det skal naturligvis overvejes, hvilke søgemønstre der – med henblik på saglige formål – må formodes at være almindeligt forekommende blandt medarbejdere i borgerservicecentre.

Hvis en søgning findes af den automatiserede overvågning, betyder det ikke i sig selv, at der er tale om et misbrug. Det betyder, at der kan være grund til at spørge den pågældende medarbejder om grunden til opslaget.

Kontrol af opslag, som finder sted på baggrund af den automatiserede overvågning, skal ske på samme måde som ved kontrol på baggrund af stikprøver af loggen med hensyn til forelæggelse for medarbejdere m.v. Medarbejderne bør også informeres om automatisk overvågning. Se eksempelboks 9.

6. Datatilsynets kontrol med datasikkerheden

Datatilsynet har mulighed for at tage stilling til, om datasikkerheden i kommunens borgerservicecenter (eller andre steder i kommunen) lever op til de regler, der er beskrevet ovenfor.

Det kan ske i forbindelse med en inspektion i kommunen. Det kan også ske i forbindelse med presseomtale, et tip fra en borger eller medarbejder eller i forbindelse med en klagesag.

En borger har mulighed for at klage over kommunens behandling af personoplysninger om vedkommende. Det gælder også datasikkerheden omkring behandlingen af personoplysningerne[20].

Når Datatilsynet har taget stilling til, om datasikkerheden er god nok, vil Datatilsynet i nogle tilfælde offentliggøre sin udtalelse på tilsynets hjemmeside.

[20] Jf. § 58, stk. 1, i persondataloven