Oversigt (indholdsfortegnelse)

Den fulde tekst

Vejledning til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning

Indledning

Denne vejledning beskriver og uddyber de tekniske og organisatoriske sikkerhedsforanstaltninger, som skal træffes i den offentlige forvaltning af hensyn til behandlingssikkerheden (datasikkerheden).

De overordnede regler for datasikkerheden er fastsat i lov om behandling af personoplysninger (persondataloven) §§ 41-42. Disse bestemmelser har følgende ordlyd:

§ 41. *Personer, virksomheder mv., der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, må kun behandle disse efter instruks fra den dataansvarlige, medmindre andet følger af lov eller bestemmelser fastsat i henhold til lov.*

Stk. 2. Den i stk. 1 nævnte instruks må ikke begrænse den journalistiske frihed eller være til hinder for tilvejebringelsen af et kunstnerisk eller litterært produkt.

Stk. 3. 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. Tilsvarende gælder for databehandlere.

Stk. 4. For oplysninger, som behandles for den offentlige forvaltning, og som er af særlig interesse for fremmede magter, skal der træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.

Stk. 5. Justitsministeren kan fastsætte nærmere regler om de i stk. 3 anførte sikkerhedsforanstaltninger.

§ 42. *Når en dataansvarlig overlader en behandling af oplysninger til en databehandler, skal den dataansvarlige sikre sig, at databehandleren kan træffe de i § 41, stk. 3-5, nævnte tekniske og organisatoriske sikkerhedsforanstaltninger, og påse, at dette sker.*

Stk. 2. Gennemførelse af en behandling ved en databehandler skal ske i henhold til en skriftlig aftale parterne imellem. Af aftalen skal det fremgå, at databehandleren alene handler efter instruks fra den dataansvarlige, og at reglerne i § 41, stk. 3-5, ligeledes gælder for behandlingen ved databehandleren. Hvis databehandleren er etableret i en anden medlemsstat, skal det fremgå af aftalen, at de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den medlemsstat, hvor databehandleren er etableret, gælder for denne.

Justitsministeren har i medfør af lovens § 41, stk. 5, udstedt bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning. Bekendtgørelsens § 2, stk. 2, er ændret ved bekendtgørelse nr. 201 af 22. marts 2001. Bekendtgørelsen indeholder nærmere regler om de sikkerhedsforanstaltninger, som kræves efter lovens § 41, stk. 3.

Bestemmelserne i bekendtgørelse nr. 528 (sikkerhedsbekendtgørelsen) er gengivet nedenfor. I tilknytning til den enkelte bestemmelse gives en beskrivelse og uddybning af de krav, som følger af bestemmelsen.

Bekendtgørelsens enkelte bestemmelser

Kapitel 1

Almindelige bestemmelser

§ 1. *Denne bekendtgørelse gælder for behandling af personoplysninger, som foretages for den offentlige forvaltning helt eller delvis ved hjælp af elektronisk databehandling.*

Bekendtgørelsen gælder alene for behandling af personoplysninger, som foretages for den offentlige forvaltning helt eller delvis ved hjælp af elektronisk databehandling. Ved en behandling, hvor kun en del foretages ved hjælp af elektronisk databehandling, gælder bekendtgørelsen kun for denne del. For den offentlige forvaltnings behandling af personoplysninger i manuelle registre samt for behandling af personoplysninger i den private sektor gælder lovens bestemmelser umiddelbart samt bestemmelser, som måtte være fastsat i selvstændige bekendtgørelser, jf. lovens § 41, stk. 5.

§ 2. *Behandling af personoplysninger skal ske i overensstemmelse med bestemmelserne i kapitel 1 og 2.*

For enhver behandling af personoplysninger, uanset om der indgår fortrolige oplysninger eller ej, gælder bestemmelserne i bekendtgørelsens kapitel 1 - almindelige bestemmelser - og i kapitel 2 - generelle sikkerhedsbestemmelser.

Stk. 2. Behandling af personoplysninger, hvor der skal ske anmeldelse til Datatilsynet efter reglerne i kapitel 12 i lov om behandling af personoplysninger, skal tillige ske i overensstemmelse med bestemmelserne i denne bekendtgørelses kapitel 3. Dette gælder dog ikke for behandling af personoplysninger, der udelukkende sker med henblik på at føre et retsinformationssystem, i det omfang der er tale om oplysninger i den offentligt tilgængelige del af retsinformationssystemet. Det gælder endvidere ikke for behandling af oplysninger om ansattes fagforeningsmæssige tilhørsforhold i forbindelse med aftaler om kontingentindeholdelse.

For behandlinger, som efter reglerne i lovens kapitel 12 skal anmeldes til Datatilsynet, gælder ud over bestemmelserne i bekendtgørelsens kapitel 1 og 2 også bestemmelserne i kapitel 3 - supplerende sikkerhedsforanstaltninger for anmeldelsespligtige behandlinger.

Reglerne for anmeldelse af behandlinger, der foretages for den offentlige forvaltning, fremgår af lovens kapitel 12 og er beskrevet i Datatilsynets vejledning nr. 125 af 10. juli 2000.

§ 3. *Den dataansvarlige myndighed skal træffe de fornødne tekniske og organisatoriske foranstaltninger mod, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lov om behandling af personoplysninger.*

Bestemmelsen er en gentagelse af lovens § 41, stk. 3, idet dog sidste punktum ikke er medtaget.

Foranstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, kan f.eks. bestå i, at der efter nærmere fastlagte rutiner foretages sikkerhedskopiering.

De sikkerhedsforanstaltninger, der er fastsat i sikkerhedsbekendtgørelsen, retter sig navnlig mod, at oplysningerne kommer til uvedkommendes kendskab, bliver misbrugt eller i øvrigt behandles i strid med loven.

En mere generelt dækkende vejledning om etablering af såvel tekniske som organisatoriske sikkerhedsforanstaltninger i forbindelse med elektronisk databehandling kan findes i Dansk Standard DS 484, Norm for edb-sikkerhed.

Stk. 2. For personoplysninger, som er af særlig interesse for fremmede magter, skal der træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.

Bestemmelsen svarer til indholdet af lovens § 41, stk. 4. Det vil påhvile den dataansvarlige myndighed først at identificere de af myndighedens behandlinger, som vedrører oplysninger af særlig interesse for fremmede magter, og derefter træffe de efter myndighedens vurdering fornødne sikkerhedsforanstaltninger.

§ 4. *Datatilsynet fører tilsyn med overholdelsen af denne bekendtgørelse og kan i den forbindelse komme med henstillinger over for den dataansvarlige myndighed vedrørende de trufne sikkerhedsforanstaltninger, jf. § 3.*

Datatilsynets tilsyn med overholdelse af bekendtgørelsen er en del af det tilsyn, som Datatilsynet efter lovens § 55 skal føre, nemlig tilsyn med enhver behandling, der omfattes af loven (med undtagelse af behandlinger, der foretages for domstolene, jf. lovens kapitel 17).

Kapitel 2

Generelle sikkerhedsbestemmelser

§ 5. *Den dataansvarlige myndighed skal fastsætte nærmere interne bestemmelser om sikkerhedsforanstaltninger i myndigheden til uddybning af de regler, der fremgår af denne bekendtgørelse. Bestemmelserne skal navnlig omfatte organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer. Der skal endvidere fastsættes instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af edb-udstyr. Desuden skal der fastsættes retningslinier for myndighedens tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for myndigheden.*

Idet bestemmelserne i bekendtgørelsen er af mere generel og overordnet karakter, vil der være behov for, at den enkelte dataansvarlige myndighed nærmere fastlægger og beskriver, hvorledes bekendtgørelsens bestemmelser er tænkt opfyldt, og i det hele taget hvorledes sikkerhedsarbejdet i forbindelse med behandling af personoplysninger tilrettelægges.

Der er i denne bestemmelse nævnt et antal emner for interne bestemmelser, instrukser og retningslinier. Opremsningen skal ses som eksempler og er ikke udtømmende.

Udover at tjene som dokumentation vil de bestemmelser mv., som den dataansvarlige myndighed udarbejder i henhold til denne bestemmelse, også kunne tjene som arbejdsgangsbeskrivelser, funktionsbeskrivelser for forskellige funktioner i sikkerhedsarbejdet, ansvarsbeskrivelse og -afgrænsning mm.

Visse af de nævnte beskrivelser kan være af en sådan karakter, at sikkerhedsmæssige hensyn taler for at klassificere dem som ikke offentligt tilgængelige. Dette kan være aktuelt for f.eks. beskrivelse af tekniske indretninger såsom alarmsystemer.

Stk. 2. De interne bestemmelser skal gennemgås mindst én gang hvert år med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold i myndigheden.

Da dokumentation er uden værdi, hvis den ikke er aktuel, bør de interne bestemmelser nævnt ovenfor løbende ajourføres, således at de til enhver tid afspejler de faktiske forhold på stedet. Efter denne bestemmelse påhviler det den dataansvarlige at kontrollere mindst en gang årligt, at den nævnte ajourføring af de interne bestemmelser er foretaget.

§ 6. *Den dataansvarlige myndighed skal give den fornødne instruktion til de medarbejdere, som behandler personoplysningerne. Medarbejderne skal herunder gøres bekendt med de regler, der er fastsat i medfør af § 5.*

For at behandlingen af personoplysninger kan ske korrekt og som forudsat af den dataansvarlige, skal medarbejdere, som udfører behandlingen, ved uddannelse, instruktion mv. bibringes den nødvendige viden. For at behandlingen kan ske sikkerhedsmæssigt korrekt, skal medarbejderne have kendskab til de gældende sikkerhedsregler, hvilket bl.a. kan opnås ved at orientere medarbejderne om relevante dele af bestemmelserne, som fastsættes efter bekendtgørelsens § 5.

§ 7. *Hvis behandling af personoplysninger foretages af en databehandler på den dataansvarliges vegne, skal der foreligge en skriftlig aftale, hvoraf det fremgår, at reglerne i denne bekendtgørelse ligeledes gælder for behandlingen ved databehandleren. Hvis databehandleren er etableret i en anden medlemsstat, skal det fremgå af aftalen, at de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den medlemsstat, hvor databehandleren er etableret, gælder for denne.*

Efter denne bestemmelse skal gennemførelse af en behandling ved en databehandler ske i henhold til en skriftlig aftale, som den dataansvarlige har indgået med databehandleren. Det skal af denne aftale fremgå, at den behandling, som den dataansvarlige overlader til databehandleren, skal ske efter reglerne i denne bekendtgørelse, helt som hvis den dataansvarlige selv havde forestået behandlingen.

Den dataansvarlige skal sikre, at behandlingen sker efter reglerne i bekendtgørelsen, selv om behandlingen sker hos en databehandler, som er etableret i en anden medlemsstat. Såfremt der i det pågældende land findes særlige sikkerhedsregler for

databehandlerens virksomhed, skal det af aftalen mellem den dataansvarlige og databehandleren fremgå, at databehandleren tillige skal iagttage disse.

Bestemmelsen sigter først og fremmest mod de situationer, hvor databehandlingen er overladt til et edb-servicebureau.

I øvrigt fremgår det af persondatalovens § 42, stk. 1, at når en dataansvarlig overlader behandling af oplysninger til en databehandler, skal den dataanvarlige sikre sig, at databehandleren kan træffe de i lovens § 41, stk. 3 - 5, nævnte tekniske og organisatoriske sikkerhedsforanstaltninger, og påse, at dette sker. Den dataansvarlige skal således aktivt sikre, at de krævede sikkerhedsforanstaltninger overholdes hos databehandleren, og det kan i den sammenhæng være relevant at indhente en årlig revisionserklæring fra en uafhængig tredjepart. Den skriftlige aftale parterne imellem som nævnt ovenfor kunne bl.a. indeholde denne revisionserklæring som en betingelse for at lade behandlingen foretage hos databehandleren.

Endelig bør det af den skriftlige aftale fremgå, om behandlingen af personoplysninger hos databehandleren sker helt eller delvist ved anvendelse af hjemmearbejdspladser.

Stk. 2. Hvis behandling af personoplysninger finder sted på en pc-arbejdsplads uden for den dataansvarlige myndigheds lokaliteter, skal myndigheden fastsætte særlige retningslinier herfor, således at det sikres, at bestemmelserne om sikkerhedsforanstaltninger iagttages.

Ved pc-arbejdspladser uden for den dataansvarliges lokaliteter tænkes der her først og fremmest på hjemmearbejdspladser (arbejdsplads som etableres ved opstilling i en medarbejders hjem af en pc med forbindelse til arbejdsgiverens edb-system, således at medarbejderen kan udføre visse arbejdsopgaver hjemmefra), men bestemmelsen vil også gælde i en række andre tilfælde, hvor behandling foretages andre steder end ved de sædvanlige arbejdspladser på arbejdsgiverens lokaliteter (brug af bærbare pc'er under rejse, hos kunder eller klienter etc., anvendelse af en pc i en anden virksomhed eller myndighed, anvendelse af privat pc i hjemmet). Dette gælder ikke alene for pc'er, men også for andet elektronisk udstyr, f.eks PDA'er (Personal Digital Assistant) og lignende.

Nedenstående betragtninger er gjort vedrørende hjemmearbejdspladser, men tilsvarende kan gøres for alle tilfælde af eksempler på arbejdspladser uden for den dataansvarliges lokaliteter. Den dataansvarlige skal foretage en vurdering ud fra de sikkerhedsmæssige forhold og fastsætte særlige retningslinier på grundlag heraf.

Ved arbejde fra en hjemmearbejdsplads finder anvendelsen af data sted i et andet miljø. Mens der i forbindelse med arbejde på den almindelige arbejdsplads gennem lang tids praksis er indarbejdet rutiner og adfærd, som sikrer en forsvarlig behandling af data, eksisterer der ikke på forhånd en tilsvarende praksis, som sikrer, at behandlingen af data fra en hjemmearbejdsplads sker med tilsvarende sikkerhed.

Der er derfor en række forhold, som der skal tages stilling til. Af de sikkerhedsmæssige problemområder, som skal vurderes, kan bl.a. nævnes:

Lokal lagring af oplysninger. Hvis det er nødvendigt, at hjemme-pc'en ikke bare anvendes som terminal mod det centrale system, men også til lagring af oplysninger fra det centrale system, bør oplysningerne krypteres.

Lokal udskrivning af oplysninger. Hvis det ikke kan undgås, at der skal udskrives oplysninger på hjemme-pc'en, skal der fastsættes regler og gives instruktion vedrørende opbevaring og tilintetgørelse af udskrifter, så oplysningerne ikke kommer uvedkommende til kendskab.

Anden anvendelse af hjemme-pc'en. Hvis den dataansvarlige tillader anden anvendelse, f.eks. til privat brug, skal der fastsættes retningslinier for denne anvendelse og etableres de nødvendige sikkerhedsforanstaltninger i forbindelse dermed.

Fysisk sikkerhed. I hjemmemiljøet må det forventes, at den fysiske sikring mod tyveri, hærværk og uvedkommendes adgang i det hele taget ikke vil være på højde med forholdene på den almindelige arbejdsplads. Særligt ved lokal lagring af oplysninger og lokal udskrivning må opmærksomheden rettes mod dette punkt. Endvidere kan muligheden for aflytning af datatransmissionen ved fysisk indgriben i telefonlinier være større i dette miljø.

Anvendelse af opkaldslinier. Hvis etablering af forbindelse fra hjemmearbejdspladsen til det centrale system sker ved anvendelse af opkaldsforbindelse (analog telefonforbindelse, ISDN, mobiltelefon etc.), skal der i denne forbindelse træffes foranstaltninger mod, at uvedkommende kan foretage opkald til det centrale system og i det hele taget gribe ind i kommunikationen. Som eksempler på sådanne foranstaltninger kan nævnes tilbagekald, passwordbeskyttelse og lukkede brugergrupper. Det kan i denne forbindelse bl.a. overvejes, om der skal være særlige tidsrum, hvor hjemmearbejdspladsen ikke kan anvendes, og om der skal etableres en særlig logning af dens anvendelse.

Der bør løbende ske en ajourføring af de særlige retningslinier vedrørende hjemmearbejdspladser for at sikre, at bestemmelserne om sikkerhedsforanstaltninger iagttages.

§ 8. *På steder, hvor der foretages behandling af personoplysninger, skal der træffes forholdsregler med henblik på at forhindre uvedkommendes adgang til oplysningerne.*

Bestemmelsen retter sig meget bredt mod lokaliteter, hvor behandling af personoplysninger finder sted, og hovedsageligt mod den fysiske sikkerhed. Forholdsreglerne, som træffes efter denne bestemmelse, kan ses som et supplement til bekendtgørelsens øvrige bestemmelser om adgang til oplysninger og vil i vid udstrækning være sammenfaldende med den dataansvarliges gængse regler om fysisk sikkerhed, såsom aflåsning af lokaler og bygningsafsnit, alarmsystem, begrænset adgang til serverrum samt placering af skærme og printere (specielt i ekspeditions- og publikumsområder).

§ 9. *I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier skal der træffes de fornødne foranstaltninger for at sikre, at bestemmelsen i § 3 iagttages.*

Foranstaltninger mod, at uvedkommende får adgang til lagrede oplysninger, vil afhænge af den konkrete situation. Ved reparation og service af udstyr, skal den dataansvarlige, hvis ikke oplysningerne kan fjernes fra udstyret, sikre sig, at reparations- og servicepersonalet vil behandle oplysninger, som de måtte blive bekendt med under deres arbejde, som fortroligt materiale, der under ingen omstændigheder må videregives eller anvendes. Ved kassation af lagringsmedier og udstyr, som indeholder personoplysninger, bør lagringsmedierne destrueres eller afmagnetiseres, så der ikke er mulighed for at læse indholdet. Hvis den dataansvarlige frem for at destruere lagringsmedier afhænder disse med henblik på genbrug, skal de lagrede oplysninger slettes effektivt ved overskrivning.

Datatilsynet anbefaler, at der til overskrivning af datamedier anvendes et specialprogram, som overskriver data flere gange i overensstemmelse med en anerkendt specifikation (f.eks. DOD 5220.22-M)

Ved reparation af udstyr skal lagrede oplysninger, så vidt det er muligt, ligeledes slettes forinden.

Inddateringsmateriale som indeholder personoplysninger

§ 10. *Inddatamateriale, som ikke indgår i en manuel sag eller i et manuelt register, må kun anvendes af personer, som er beskæftiget med inddatering. Inddatamateriale, som er omfattet af bestemmelsen i § 2, stk. 2, skal opbevares aflåst, når det ikke anvendes.*

Ved inddatamateriale forstås det grundmateriale (papirbaseret eller elektronisk), hvorfra der hentes oplysninger til videre elektronisk databehandling. Bestemmelsen gælder for inddatamateriale, som hverken indgår i en traditionel, papirbaseret sag, herunder en patientjournal, eller i et manuelt register. Således vil modtagne ansøgningsblanketter, som opbevares samlet uden at være journaliseret på f.eks. en sag vedrørende den enkelte ansøger eller på en fælles sag vedrørende den pågældende type af ansøgning, være omfattet af bestemmelsen, hvis blanketterne skal inddateres elektronisk. Derimod vil ansøgningsblanketterne ikke være omfattet af bestemmelsen, så snart den omtalte journalisering er foretaget, ligesom de heller ikke vil være omfattet, hvis de opbevares på en sådan måde, at de må siges at udgøre et manuelt register (f.eks. ordnet efter særlige kriterier i et ringbind), idet bekendtgørelsen ikke gælder for manuelle registre.

Inddatamateriale i elektronisk form, f.eks. transaktioner opsamlet i en fil, vil normalt være omfattet af bestemmelsen.

Det skal bemærkes, at inddatering ved indtastning, f.eks. i et on-line system, i sig selv udgør en behandling, der er omfattet af bekendtgørelsen.

Inddatamateriale, som er omfattet af bestemmelsen i § 2, stk. 2, dvs. materiale, der som hovedregel indeholder oplysninger af fortrolig karakter, skal med henblik på at hindre uvedkommendes adgang til oplysningerne opbevares aflåst, når det ikke benyttes. Der stilles ikke mere specifikke krav om, hvorledes aflåsning skal etableres, men det forudsættes, at det sker ved aflåsning af skuffe, skab, lokale eller på anden måde, som efter den dataansvarliges vurdering er forsvarlig.

Stk. 2. Inddatamateriale som nævnt i stk. 1 skal slettes eller tilintetgøres, når det ikke længere skal anvendes til de formål, som behandlingen varetager, eller til kontrol med de inddaterede personoplysninger, dog senest efter en af den dataansvarlige myndighed nærmere fastsat frist.

Inddateringsmateriale, som nævnt i stk. 1 - bestemmelsen gælder altså ikke for materiale, som indgår i en manuel sag eller i et manuelt register - skal slettes (materiale i elektronisk form) eller tilintetgøres (papirbaseret materiale), når der ikke længere er brug for materialet. Den dataansvarlige må således i forbindelse med hver enkelt behandling tage stilling til, hvor længe der er

behov for eller krav om, at inddateringsmaterialet opbevares, og formelt fastsætte en seneste frist for sletning eller tilintetgørelse.

Stk. 3. Ved tilintetgørelse af inddatamateriale skal der træffes de fornødne sikkerhedsforanstaltninger mod, at materialet misbruges eller kommer til uvedkommendes kendskab.

En procedure for tilintetgørelse af inddatamaterialet skal efter bestemmelsen tilrettelægges på en sådan måde, at materialet ikke i denne sammenhæng kan misbruges eller komme uvedkommende til kendskab. Der kan i denne forbindelse f.eks. være tale om at opsamle materiale i aflåste containere med efterfølgende anvendelse af en pålidelig makuleringsservice for fortroligt materiale.

Autorisation og adgangskontrol

§ 11. *Kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles.*

I persondataloven er det i kapitel 11 om behandlingssikkerhed anført, at der skal træffes de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod bl.a., at oplysningerne kommer til uvedkommendes kendskab (§ 41, stk. 3). Det er derfor i denne bestemmelse i bekendtgørelsen fastsat, at der kun må gives adgang til personoplysningerne for personer, som direkte er autoriserede hertil. Det forudsættes, at der fastlægges en formel autorisationsordning og -arbejdsgang.

Stk. 2. 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.

I denne bestemmelse fastslås det, at der kun må autoriseres personer, der er beskæftiget med de formål, hvortil oplysningerne behandles. Alle andre personer, også øvrige medarbejdere hos den dataansvarlige myndighed, er i forbindelse med den omhandlede behandling uvedkommende og må ikke have adgang til oplysningerne. Tilsvarende betragtninger ligger bag begrænsningen i autorisationen til kun at omfatte anvendelser, som de enkelte brugere har behov for. Det forudsættes, at der i den formelle autorisationsprocedure vil indgå en forudgående vurdering af, hvad den enkelte bruger har behov for at være autoriseret til. I den formelle autorisationsprocedure kan endvidere f.eks. indgå, at der til den pågældende bruger fremsendes et brev, hvori det nærmere beskrives, hvilke oplysninger brugeren herved autoriseres (godkendes) til at anvende.

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, eller hvis ansættelsesforhold ophører.

Stk. 3. Der må endvidere autoriseres personer, for hvem adgang til oplysninger er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.

Udover til de ovenfor omhandlede medarbejdere i den pågældende myndighed kan det være aktuelt at give adgang til oplysninger til personer, som ikke er direkte vedkommende i forhold til den enkelte behandling, men som i anden sammenhæng har behov herfor. Der er i denne bestemmelse tænkt på sådanne personer, som udfører revision, og personer som udfører teknisk vedligeholdelse, driftsovervågning, fejlretning mv. Den dataansvarlige skal fastlægge særlige retningslinier for udstedelse af sådanne autorisationer og for inddragelse heraf for så vidt angår autorisationer, der kun behøver at være midlertidige (f.eks. autorisationer til brug ved en årlig revision).

§ 12. *Der skal træffes foranstaltninger for at sikre, at kun autoriserede brugere kan få adgang, og at disse kun kan få adgang til de personoplysninger og anvendelser, som de er autoriserede til.*

Udover den ovenfor omtalte formelle autorisation af brugere skal der etableres en teknisk adgangskontrol i systemerne, således at autoriserede personer skal identificere sig over for systemet for at få adgang til at foretage behandlinger i overensstemmelse med autorisationen. Den mest almindelige form for adgangskontrol er brugeridentifikation med tilhørende password, men andre former for adgangskontrol er ikke udelukket. Såfremt password benyttes, skal den dataansvarlige fastsætte nærmere retningslinier for behandling og opbygning af password.

Datatilsynet anbefaler, at password har en længde på mindst 8 tegn. Passwords bør opbygges af en blanding af tal og store og små bogstaver. Password bør skiftes mindst en gang om året.

Uddatamateriale som indeholder personoplysninger

§ 13. *Uddatamateriale må kun anvendes af personer, der er beskæftiget med de formål, til hvilke behandlingen af personoplysningerne foretages.*

Ved uddatamateriale forstås det resultat af en elektronisk databehandling, som foreligger på papirbaseret eller elektronisk form. Bestemmelserne i § 13, stk. 1 - 5, gælder kun for uddatamateriale - på papir eller i elektronisk form - der indeholder personoplysninger, og således ikke for f.eks. anonyme oversigter og lignende. Bestemmelserne gælder endvidere kun for uddatamateriale - på papir eller i elektronisk form - som ikke indgår i en manuel sag eller i et manuelt register, jf. stk. 6.

Idet personoplysninger ikke må komme uvedkommende til kendskab, må uvedkommende heller ikke få adgang til uddatamateriale, som indeholder personoplysninger. Adgangen til sådant uddatamateriale skal derfor begrænses til personer, som er beskæftiget med de formål, til hvilke behandlingen af personoplysningerne foretages.

Stk. 2. Herudover må uddatamateriale anvendes af personer, som er beskæftiget med revision eller drifts- og systemtekniske opgaver i det pågældende system.

Det kan også være aktuelt at give adgang til uddatamateriale for personer, som ikke er direkte beskæftiget med den pågældende behandling, men som i anden sammenhæng har behov herfor. Der er i denne bestemmelse tænkt på sådanne personer, som udfører revision, og personer som udfører teknisk vedligeholdelse, driftsovervågning, fejlretning mv.

Stk. 3. Uddatamateriale skal opbevares på en sådan måde, at uvedkommende ikke kan få adgang til at gøre sig bekendt med de personoplysninger, som er indeholdt heri.

Hvorledes uddatamateriale kan opbevares, så uvedkommende ikke kan gøre sig bekendt med personoplysningerne deri, vil afhænge af den konkrete situation. Ansvaret for forsvarlig opbevaring påhviler den dataansvarlige, og denne bør fastsætte formelle retningslinier herfor.

Stk. 4. Uddatamateriale skal slettes eller tilintetgøres, når det ikke længere skal anvendes til de formål, som behandlingen varetager, og senest efter en af den dataansvarlige myndighed nærmere fastsat frist.

Uddatamateriale som nævnt i bemærkningerne til bestemmelsen i stk. 1 skal slettes (materiale i elektronisk form) eller tilintetgøres (papirbaseret materiale), når der ikke længere er brug for materialet. Den dataansvarlige skal derfor i forbindelse med hver enkelt behandling tage stilling til, hvor længe der er behov for eller krav om, at uddatamaterialet opbevares, og formelt fastsætte en seneste frist for sletning eller tilintetgørelse.

Stk. 5. Ved tilintetgørelse af uddatamateriale skal der træffes de fornødne sikkerhedsforanstaltninger mod, at materialet misbruges eller kommer til uvedkommendes kendskab.

En procedure for tilintetgørelse af uddatamaterialet skal efter bestemmelsen tilrettelægges på en sådan måde, at materialet ikke i denne sammenhæng kan misbruges eller komme uvedkommende til kendskab. Der kan f.eks. være tale om at opsamle materiale i aflåste containere med efterfølgende anvendelse af en pålidelig makuleringsservice for fortroligt materiale.

Stk. 6. Bestemmelserne i stk. 1-5 gælder ikke for uddatamateriale, som indgår i en manuel sag eller i et manuelt register.

Sikkerhedsbekendtgørelsen gælder ikke for de nævnte situationer. For materiale, som indgår i en manuel sag, gælder forvaltningslovens regler, mens manuelle registre er omfattet af bestemmelserne i persondataloven herunder reglerne om behandlingssikkerhed i §§ 41-42, samt af særlige regler, der måtte være fastsat for manuelle registre.

Eksterne kommunikationsforbindelser

§ 14. *Der må kun etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.*

Bestemmelsen gælder enhver form for telekommunikation i forbindelse med behandling af personoplysninger, f.eks. forsendelse af oplysninger med telefax eller ekstern e-post, etablering af terminaladgang ved opkaldsmodem, adgang til oplysninger via myndighedens hjemmeside og etablering af internetadgang fra arbejdspladser på myndighedens interne net. De særlige sikkerhedsforanstaltninger skal træffes efter myndighedens vurdering af sikkerhedsrisici i det konkrete tilfælde, herunder med hensyntagen til karakteren af de omhandlede oplysninger.

For at kunne fastlægge sikkerhedsniveauet er det nødvendigt, at den dataansvarlige foretager en samlet risikovurdering, som omfatter alle elementer i kommunikationsforbindelsen.

Ved tilslutning til **Internet** eller andre åbne net skal der træffes foranstaltninger, som sikrer imod uvedkommende trafik og forhindrer adgang fra det åbne net til den dataansvarliges interne net.

Ved brug af **telefax** skal opmærksomheden særligt været rettet mod dels risikoen for at faxen sendes til forkert modtager, dels at den modtagne fax kan være tilgængelig for uvedkommende hos modtageren.

Ved afsendelse af faxer skal det angivne telefaxnummer kontrolleres nøje. Anvendelse af fastindkodede telefaxnumre (kortvalg) kan ligeledes overvejes.

For så vidt angår behandlingen af modtagne faxer bør telefaxmaskinen placeres således, at uvedkommende ikke umiddelbart har adgang til modtagne faxer. Ved anvendelse af telefax i forbindelse med mere følsomme oplysninger kan en løsning være at anvende udstyr, som lagrer modtagne faxer i maskinen, og kun lade specielt autoriserede medarbejdere udskrive dem.

Ved transmission af personoplysninger over **opkaldsforbindelser** (via analog telefonforbindelse, ISDN, mobiltelefon etc.), f.eks. ved etablering af terminaladgang til et centralt system fra en bærbar pc, skal der specielt træffes foranstaltninger mod, at uvedkommende kan foretage opkald. Det kan bl.a. være relevant at anvende faciliteter som tilbagekald eller lukkede brugergrupper.

For transmission af personoplysninger over **åbne net** (f.eks. Internet) gælder konkret nedenstående minimumskrav om sikkerhedsforanstaltninger:

Ved transmission af oplysninger over det åbne Internet er der generelt en risiko for, at oplysningerne undervejs læses og endog ændres af uvedkommende. Derudover er der en risiko for, at parterne i kommunikationen ikke er dem, de udgiver sig for.

Disse risici må vurderes af den dataansvarlige i den konkrete situation, således at der kan træffes de fornødne sikkerhedsforanstaltninger.

Hvad angår fortrolighed kan denne sikres ved forsvarlig kryptering af de transmitterede oplysninger. Hvis der er tale om transmission af fortrolige oplysninger, herunder personnummer, skal der som minimum foretages en kryptering. Hvis de transmitterede oplysninger er af følsom karakter (omfattet af persondatalovens § 7, stk. 1 og § 8, stk. 1), skal der anvendes en stærk kryptering, baseret på en anerkendt algoritme.

Sikkerhed for autenticitet (afsenders og modtagers identitet) og integritet (de transmitterede oplysningers ægthed) må sikres i fornødent omfang ved anvendelse af passende sikkerhedsforanstaltninger, f.eks. elektronisk signatur eller individuelle, fortrolige adgangskoder.

Kapitel 3

Supplerende sikkerhedsforanstaltninger for anmeldelsespligtige behandlinger

§ 15. *Bestemmelserne i kapitel 3 finder ikke anvendelse i det omfang de behandlede oplysninger ikke i sig selv ville være omfattet af anmeldelsespligt til Datatilsynet.*

Behandlinger, som omfatter oplysninger af fortrolig karakter, er som hovedregel anmeldelsespligtige og skal ske under iagttagelse af de supplerende sikkerhedsbestemmelser i dette kapitel. Se nærmere om anmeldelsespligten i Datatilsynets vejledning nr. 125 af 10. juli 2000.

Udover disse oplysninger af fortrolig karakter, som indgår i en anmeldelsespligtig behandling, vil der typisk i behandlingen også indgå oplysninger, som ikke er af fortrolig karakter. Bestemmelserne i dette kapitel gælder ikke for anvendelse af disse ikke-fortrolige oplysninger og heller ikke for anvendelse af de fortrolige oplysninger, som efter lovens undtagelsesbestemmelser kan indgå i en behandling, uden at behandlingen er anmeldelsespligtig.

Det vil f.eks. gælde for en anmeldelsespligtig behandling, hvori der indgår oplysninger om personers helbredsforhold, at alle anvendelse af oplysningerne om helbredsforhold skal logges efter denne bekendtgørelses § 19, stk. 1. Derimod vil anvendelse af ikke-fortrolige oplysninger såsom personers adresse ikke skulle logges. Det er dog en forudsætning, at en sådan anvendelse af ikke-fortrolige oplysninger ikke indirekte kan afsløre fortrolige forhold vedrørende de berørte personer.

De detaljerede undtagelsesbestemmelser og dermed beskrivelse af de oplysninger af fortrolig karakter, som kan indgå i en behandling, uden at den bliver anmeldelsespligtig, findes i lovens § 44, stk. 1, samt i Justitsministeriets bekendtgørelse nr. 529

af 15. juni 2000 om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for den offentlige forvaltning, fastsat i henhold til lovens § 44, stk. 2, og § 44, stk. 4.

Autorisation og adgangskontrol

§ 16. *Autorisationer, jf. § 11, skal angive, i hvilket omfang brugeren må forespørge, inddatere eller slette personoplysninger.*

Udover de generelle krav i § 11 vedrørende autorisation af brugere kræves det i forbindelse med anmeldelsespligtige behandlinger, at myndigheden konkret tager stilling til, hvorvidt en bruger kun skal kunne foretage forespørgsler, eller om brugeren også skal kunne inddatere oplysninger, samt om brugeren skal kunne slette oplysninger. Såfremt der er brugere, som kun skal autoriseres til enkelte af de nævnte funktioner, skal systemerne være teknisk indrettet således, at brugerne kun gives mulighed for adgang til oplysningerne i overensstemmelse med de givne autorisationer.

Når den tekniske adgangskontrol til systemets oplysninger og anvendelser heraf er baseret på brugeridentifikation med tilhørende password, skal den enkelte bruger tildeles et personligt og fortroligt password.

Det personlige og fortrolige password er knyttet til den tilhørende brugeridentifikation og må kun være kendt af den pågældende bruger. Der kan således ikke anvendes en fælleskode, dvs. én brugeridentifikation med tilhørende password, som anvendes af flere brugere.

§ 17. *Det skal sikres, at de autoriserede personer fortsat opfylder betingelserne i § 11, stk. 2 og 3, og § 16.*

Autoriserede brugere må til enhver tid kun være autoriserede til anvendelser, de har brug for. Der må derfor være tilrettelagt arbejdsgange, som sikrer, at der tilgår funktionen, som administrerer autorisationerne, oplysning om ændring af brugeres behov for autorisation, herunder oplysning om medarbejderes fratræden eller flytning inden for organisationen, således at de udstedte autorisationer kan blive ændret eller inddraget.

Stk. 2. Kontrol heraf skal foretages mindst en gang hvert halve år.

Efter denne bestemmelse skal der mindst en gang hvert halve år foretages kontrol af, at autorisationer ajourføres som foreskrevet ovenfor. Det er den dataansvarliges ansvar, at der fastlægges en passende kontrolprocedure. Denne procedure kan f.eks. indebære, at der i systemerne dannes en statistik over den enkelte brugers anvendelse af systemet, således at det kan konstateres, om der er udstedte autorisationer, som ikke er anvendt, og som derfor eventuelt bør inddrages.

Det er efter sikkerhedsbekendtgørelsen nu ikke længere et krav, at der udarbejdes en benyttelsesstatistik.

Kontrol med afviste adgangsforsøg

§ 18. *Der skal foretages registrering af alle afviste adgangsforsøg. Hvis der inden for en fastsat periode er registreret et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg fra samme arbejdsstation eller med samme brugeridentifikation, skal der blokeres for yderligere forsøg. Der skal løbende ske opfølgning i myndigheden.*

Bestemmelsen indebærer, at der skal foretages en registrering af ethvert afvist forsøg på adgang til systemet, uanset om afvisningen er forårsaget af brug af forkert password, forkert brugeridentifikation, manglende autorisation til en vis funktion eller andet. Herved etableres et redskab for systemadministrationen til eventuelt at afdække forsøg på uberettiget adgang til oplysningerne. Bestemmelsen indebærer endvidere, at systemet skal udvise en reaktion, således at yderligere forsøg på adgang, f.eks. efter et vist antal forsøg på at gætte password, forhindres. Denne reaktion kan være i form af lukning af den anvendte brugeridentifikation, lukning af pc'en eller adgang til lokalnettet. Reaktionen skal endvidere være af en sådan art, at hændelsen kommer til rette vedkommendes, f.eks. systemadministrationens, kendskab.

Logning

§ 19. *Der skal foretages maskinel registrering (logning) af alle anvendelser af personoplysninger. Registreringen skal mindst indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes. Myndigheder med et særligt behov kan opbevare loggen i op til 5 år.*

Efter bestemmelsen skal der som udgangspunkt foretages logning af alle anvendelser af personoplysningerne, som sker i behandlingen, jf. dog § 15. Herudover indeholder stk. 2 - 6 visse undtagelser fra det generelle logningskrav.

Ved »alle anvendelser af personoplysninger« skal her forstås de anvendelser, som foretages af brugere af systemet i forbindelse med deres arbejde. Der er en række aktiviteter i forbindelse med driftsafvikling, som indebærer overvågning af og indgriben i systemerne af drifts- og systemmedarbejdere. Anvendelser af personoplysninger i forbindelse med sådanne aktiviteter er ikke omfattet af logningskravet.

Logningen skal bl.a. omfatte en angivelse af den person, som de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Foretages der en søgning på en person ved angivelse af personnummer, skal således det anvendte personnummer eller anden entydig identifikation af den pågældende person registreres i loggen. Hvis der søges på fødselsdato, skal den angivne dato (søgekriteriet) registreres i loggen, men der er ikke krav om registrering af identifikation af de enkelte personer, som indgår i søgeresultatet, dvs. alle fundne personer med den angivne fødselsdato. Angivelsen i loggen af det anvendte søgekriterium giver mulighed for efterfølgende at rekonstruere behandlingen, herunder hvilke personer som indgik i behandlingen, hvilket bl.a. er formålet med logningen.

Der er ikke krav om udskrivning af loggen, ligesom der ikke er krav om, at loggen i den foreskrevne opbevaringstid befinder sig i det pågældende system; der er intet til hinder for, at loggen f.eks. overføres til bånd og opbevares i arkiv.

Det angives i bestemmelsen, at loggen skal opbevares i seks måneder, hvorefter den skal slettes. Sletning af loggen kan tilrettelægges således, at den foretages ved f.eks. månedlige kørsler.

Der åbnes mulighed for, at myndigheder med særlige behov kan opbevare loggen i op til fem år, men der forudsættes i så fald et særligt behov for at have oplysningerne i loggen til rådighed med henblik på anvendelse i overensstemmelse med loggens egentlige formål, nemlig at tjene som et værktøj til brug ved efterforskning i forbindelse med mulig uberettiget anvendelse af oplysningerne. Loggen kan således ikke opbevares længere end de nævnte seks måneder med henblik på anvendelse i forbindelse med de administrative opgaver, som varetages i den pågældende behandling.

Stk. 2. Bestemmelsen i stk. 1 finder ikke anvendelse for personoplysninger, som indgår i tekstbehandlingsdokumenter og lignende, der ikke foreligger i endelig form. Det samme gælder sådanne dokumenter, som foreligger i endelig form, hvis der sker sletning inden for en af den dataansvarlige myndighed nærmere fastsat kortere frist.

Bestemmelsen om logning gælder ikke den behandling af personoplysninger, som sker, når oplysningerne indgår i tekstbehandlingsdokumenter, regneark og lignende, så længe disse dokumenter er under udarbejdelse eller fungerer som arbejdsdokumenter, hvori der løbende tilføjes nye oplysninger i forbindelse med behandlingen af den enkelte sag.

Undtagelsen finder derimod ikke anvendelse, hvis myndigheden på et sagsområde har etableret en rutinemæssig administration, der ved hjælp af tekstbehandling, regneark eller lignende baseres på en behandling, som har karakter af føring af et edb-register. F.eks. gælder undtagelsen ikke en løbende notering af udbetalte ydelser eller føring af ventelister.

Bestemmelsen om logning gælder ikke færdige dokumenter og lignende, som opbevares en vis kortere periode, inden de - f.eks. efter en fastlagt arbejdsgang - enten slettes eller anonymiseres ved, at alle identifikationsoplysninger, der kan henføre oplysningerne til bestemte personer, fjernes. Den dataansvarlige skal tage stilling til længden af den omtalte kortere periode, der generelt bør være af en størrelsesorden på højst en måned, og udfærdige retningslinier for, hvorledes medarbejderne skal forholde sig.

Det skal bemærkes, at der intet er til hinder for, at færdige dokumenter ikke slettes, men overføres til et dokumentarkiv med henblik på opbevaring i længere tid. I dette tilfælde vil der imidlertid også være tale om en behandling, som vil være omfattet af bestemmelsen om logning.

Stk. 3. Bestemmelsen i stk. 1 finder ikke anvendelse, hvis behandlingen af personoplysninger udelukkende sker ved afvikling af programmer, som foretager en forud defineret massebehandling af personoplysninger (»batch«-kørsler). Der skal dog foretages maskinel logning af bruger og tidspunkt for behandlingen.

Bestemmelsen om logning gælder ikke den behandling af personoplysninger, som sker udelukkende ved afvikling af programmer, som foretager en forud defineret massebehandling af oplysningerne, såkaldte batch-kørsler. Som eksempel herpå kan nævnes (regelmæssig) opdatering af store databaser; det skal ved en sådan behandling således ikke logges, hvilke databaseregistreringer, der er blevet opdateret, dvs. hvilke af de registrerede personer der er blevet berørt af opdateringen. Det skal dog maskinelt registreres (logges), at en sådan opdateringskørsel har fundet sted, hvilken bruger der har iværksat kørslen og tidspunktet herfor.

Stk. 4. Bestemmelsen i stk. 1 finder endvidere ikke anvendelse, hvis behandlingen af personoplysningerne udelukkende sker med henblik på statistiske eller videnskabelige undersøgelser, og identifikationsoplysningerne forinden enten er krypteret eller erstattet med et kodenummer eller lignende. Der skal dog foretages maskinel logning af bruger og tidspunkt for behandlingen.

Bestemmelsen om logning gælder ikke behandling af personoplysninger, som udelukkende sker med henblik på statistiske eller videnskabelige undersøgelser. Det er dog en forudsætning, at alle identifikationsoplysninger (personnummer, navn, adresse etc.) enten kun indgår i behandlingen i krypteret form eller er erstattet af et kodenummer eller lignende. Det skal dog maskinelt registreres (logges), at en sådan behandling har fundet sted, hvilken bruger der har iværksat den og tidspunktet herfor.

Stk. 5. Bestemmelsen i stk.1 finder endelig ikke anvendelse for personoplysninger, som i form af måle- eller analyseresultater automatisk lagres i medicoteknisk udstyr. Undtagelsen omfatter tillige personoplysninger, som manuelt registreres i medicoteknisk udstyr til supplering af automatisk lagrede oplysninger.

Bestemmelsen om logning gælder ikke den behandling af personoplysninger, som sker ved automatisk registrering af måle- og analyseresultater i medicoteknisk udstyr og heller ikke for de personoplysninger, der måtte blive manuelt registreret til supplering af de automatisk registrerede oplysninger.

Datatilsynet, den 2. april 2001

Hugo Wendler Pedersen

/Ib Alfred Larsen