NOTAT

Retningslinjer

DANSKE REGIONER

26-10-2010

Sag nr. 09/2825

Anmeldelse til Datatilsynet i forbindelse med forsker-initieret sundhedsforskning i regionerne.

Datatilsynet skelner ved anmeldelse af forskningsprojekter mellem forskning i regionen (offentlig forskning) og privat forskning – se evt. www.datatilsynet.dk.

Sundhedsforskning anmeldes som offentlig forskning

Al forsker-initieret anmeldelsespligtig sundhedsforskning, der foretages i regi af regionen, skal anmeldes som offentlig forskning. Dermed registreres denne forskning, via regionernes kontaktperson, under regionens paraplyanmeldelse for sundhedsfaglig forskning ved Datatilsynet.

Hvis et projekt foregår i flere regioner, udnytter data fra landsdækkende registre m.v., skal projektet anmeldes til den dataansvarlige region. Dette vil sædvanligvis være den region, hvor den koordinerende forsøgsansvarlige har sit virke.

Offentlig forskning

Offentlig forskning skal registreres i den dataansvarlige regions relevante system. Der er metodefrihed, og regionerne kan have forskellige fremgangsmåder.

Forskeren skal sikre, at de nødvendige tiltag er gjort for at sikre data i henhold til sikkerhedsbekendtgørelsen (Bekg. nr. 528 af 15. juni 2000). De enkelte regioner bør have lokale regler, instrukser og/eller hjælpemidler, der letter den praktiske gennemførelse af dette. Såfremt der benyttes en ekstern

databehandler, skal der indgås en databehandleraftale mellem regionen og den pågældende databehandler.

Grundlæggende gælder det for offentlig forskning, at der skal benyttes et databehandlingsværktøj, der foretager transaktionslogning, såfremt det er nødvendigt at fastholde identifikationsoplysningerne i datamaterialet. Derimod anses det for tilstrækkeligt at foretage adgangslogning, hvis identifikationsoplysningerne forinden enten er krypteret eller erstattet med et løbenummer eller lignende. Denne krypterings-/kodenøgle opbevares adskilt og sikret fra datagrundlaget, således at kun enkelte personer kan få adgang til den.

Privat forskning

Anmeldelse af privat forskning skal foretages direkte til Datatilsynet. Datatilsynets vilkår, som de fremgår af Datatilsynets godkendelse, skal overholdes. Herunder skal der også, såfremt der benyttes en ekstern databehandler, udformes en databehandleraftale med den pågældende databehandler.

Hvis regionens faciliteter (pc'er, servere, drev, frysere, køleskabe etc.) benyttes til projekter, hvor regionen ikke er dataansvarlig, skal der indgås en databehandleraftale mellem den dataansvarlige for projektet og den pågældende region.

Anmeldelse til Datatilsynet af databehandling i forbindelse med forsker-initieret sundhedsforskning i regionerne

NOTAT

DANSKE REGIONER

Bilag 1

26-10-2010
Sag nr. 09/2825
Dokumentnr. 27914/10

Baggrund

Indledning
Anmeldelse til Datatilsynet af databehandling i forbindelse med forskerinitieret sundhedsforskning i regionerne er regionernes ansvar. Dansk sundhedsforskning er i mange tilfælde i international topklasse og regionerne arbejder for at fjerne barrierer for sundhedsforskningen. Uklar eller ikke enslydende vejledning kan være en barriere for forskerne.

Regionerne har ansvar for, at reglerne i persondataloven overholdes i de henseender, hvor de er dataansvarlige og databehandlere. Persondataloven handler om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger.

En vejledning skal sikre, at rådgivning af danske sundhedsforskere i regionerne for så vidt angår anmeldelse til Datatilsynet sker på baggrund af enslydende retningslinjer. Den skal sikre, at sundhedsforskere i regionerne rådgives så enslydende som muligt om, hvorvidt et forskningsprojekt skal anmeldes som offentlig eller privat sundhedsforskning. Vejledningen skal også sikre, at data, som regionen har ansvar for, behandles efter lovens forskrifter. Anmeldelse af et forskningsprojekt som enten offentligt eller privat/personligt har forskellige konsekvenser for både region og forsker.

Ved regionernes dannelse blev proceduren for anmeldelser til Datatilsynet ændret. Hovedtrækket i den ændrede procedure er, at anmeldelsen til Datatilsynet af den offentlige sundhedsforskning sker årligt fra centralt hold via en kontaktperson i regionerne. Regionernes rolle og ansvar forstærkes deraf.

Ordforklaring

Regionerne er dataansvarlige, når det drejer sig om den offentlige sundhedsforskning, der foregår i regi af regionerne. Ansvaret for anmeldelse, anvendelse og omgang med data i den offentlige sundhedsforskning påhviler regionen.

Nedenstående ordforklaringer udspringer i videst muligt omfang af Datatilsynets ordforklaring - som kan findes på www.Datatilsynet.dk – og andre officielle kilder.

Sundhedsforskning: Sundhedsforskning bruges her som den bredeste term, inkluderende alle typer af sundhedsvidenskabelig forskning, herunder basalforskning, strategisk forskning, anvendelsesorienteret forskning, klinisk forskning, sundhedstjenesteforskning mv. Sundhedsforskning defineres her som forskning rettet mod sygdomsforståelse, diagnostik, behandling, pleje, rehabilitering og forebyggelse af sygdomme, herunder forskning omfattende organisering og finansiering af disse indsatser.

Logning: Paragraf 19, stk. 1 i Sikkerhedsbekendtgørelsen siger, at 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.

Data: Ved data forstås oplysninger om identificerbare personer enten i form af biologiske prøver (eksempelvis i frysere); data i it-mæssig betydning, hvor oplysninger ligger på servere og i databaser; eller oplysninger på papir eller andre medier.

Sletning af data: Når et forskningsprojekt er afsluttet, skal alle personoplysninger slettes eller anonymiseres. Det fremgår af Datatilsynets godkendelse, hvornår sletningen skal ske. Hvis projektet også omfatter blod- eller vævsprøver, videooptagelser el.lign., skal også dette materiale destrueres, slettes eller anonymiseres ved projektets afslutning. Elektroniske forskningsdata kan i stedet afleveres til Dansk Data Arkiv. Dansk Data Arkiv indhenter, bevarer og udleverer forskningsdata fra samfundsvidenskab, sundhedsvidenskab og historie. Se evt. http://www.sa.dk/dda/

Anonyme data: Ved anonyme data forstås – i modsætning til personhenførbare data - data, hvor nøglen til at gøre data personhenførbare uigenkaldeligt er slettet og det i øvrigt ikke på anden vis er muligt at identificere personen.

Pseudonymiserede data: Ved pseudonymiserede data forstås data, hvor nøglen til at gøre data personhenførbare er tilstede, men opbevares adskilt fra data.

Dataansvarlig: Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger.

Databehandler: Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne.

Procedure for anmeldelse til Datatilsynet for den henholdsvis offentlige som private/personlige sundhedsforsker

Procedure for anmeldelse – offentlig sundhedsforsker

Den enkelte forsker/den forskningsansvarlige/afdelingen tager kontakt til den/de medarbejdere i den pågældende region, som varetager opgaven med at vurdere og registrere regionens forskningsprojekter.

Kontakten indledes typisk med en beskrivelse af projektet, og det drøftes, hvordan projektet gennemføres med fokus på behandling af data (opbevaring, adgang, logning, anonymisering/sletning m.v.). Der udleveres evt. en tjekliste med forhold, som den/de projektansvarlige skal være opmærksomme på.

Herefter registreres projektet i regionens database/på listen med minimum følgende oplysninger: projektets titel (evt. formålsbeskrivelse), om der indgår biobank i projektet, på hvilket sygehus/afdeling projektet gennemføres, projektets start- og sluttidspunkt, samt oplysning om hvorvidt projektet er afsluttet og oplysninger er slettet/anonymiseret/overført til arkiv.

Et udtræk af regionens forskningsdatabase/-liste skal sendes til Datatilsynet én gang årligt. Alle projekter på listen er omfattet af paraplyanmeldelsen til Datatilsynet.

Procedure for anmeldelse – privat sundhedsforsker

Den enkelte forsker retter selv henvendelse til Datatilsynet via tilsynets hjemmeside. På Datatilsynets hjemmeside findes vejledning om, hvilke projekter der skal anmeldes og hvordan anmeldelse rent praktisk skal foregå – via en blanket.

Efter en gennemgang af anmeldelsen udsteder Datatilsynet en tilladelse til forskeren med vilkårene for projektet. Vilkårene fastsættes til beskyttelse af deltagernes privatliv og skal sikre, at personoplysningerne behandles i overensstemmelse med loven. Datatilsynets tilladelse er tidsbegrænset. Udløbsdatoen fremgår af tilladelsen.

På Datatilsynets hjemmeside findes et link til tilsynets standardvilkår for forskningsprojekter. Disse standardvilkår er knyttet til tilladelsen.

NOTAT

DANSKE REGIONER

26-10-2010

Sag nr. 09/2825

Dokumentnr. 27922/10

Bilag 2

Lovgivning

Anmeldelsespligtig behandling (inkl. indsamling, opbevaring, håndtering og sletning) af data er underlagt lovgivning for blandt andet at beskytte følsomme personoplysninger.

Lovgivning sikrer, at borgerne kan lade bl.a. sundhedspersonale og forskere anvende deres data i forskningsmæssigt og helbredelsesmæssigt øjemed, uden at uvedkommende får kendskab til deres følsomme oplysninger eller at data (mis)bruges til andet formål end det godkendte. Samtidigt sikrer lovgivningen, at bl.a. forskere og sundhedspersonale på sikker og reguleret vis har adgang til oplysninger, der kan bidrage til forskningen og til behandlingen af den enkelte borger.

I dette bilag gives et sammenlignende overblik over central lovgivning, der har betydning for anmeldelsespligtig forskning i henholdsvis offentlig og privat regi.

Følsomme personoplysninger

I henhold til regionernes godkendelse fra Datatilsynet, er **det tilladt**, i nødvendigt omfang, at behandle følgende typer oplysninger:

- Racemæssig eller etnisk baggrund
- Religiøs overbevisning
- Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol m.v.
- Seksuelle forhold
- Strafbare forhold
- Væsentlige sociale problemer

Der foreligger således **ikke tilladelse** til at behandle oplysninger om:

- Politisk overbevisning
- Filosofisk overbevisning
- Fagforeningsmæssige tilhørsforhold

Sammenligning af regler	**Offentlig forskning**	**Privat forskning**
Reference	**persondataloven**, **sikkerhedsbekendtgørelsen** og **vejledning til sikkerhedsbekendtgørelsen** Det primære grundlag for problemstillingen, der behandles her er **persondatalovens** § 41 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. Der er flere steder i sikkerhedsbekendtgørelsen henvisning til dennes § 2 stk. 2. **Sikkerhedsbekendtgørelsen** § 2. Behandling af personoplysninger skal ske i overensstemmelse med bestemmelserne i kapitel 1 og 2. 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.	**persondataloven** og **standardvilkår for forskningsprojekter** Det primære grundlag for problemstillingen, der behandles her er **persondatalovens** § 41 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.
Generelt	**Sikkerhedsbekendtgørelsen § 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.	Det fremgår af lovens § 41, stk. 3, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysningerne hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.
Personfølsomme data uden pseudonymisering og/eller kryptering	**Sikkerhedsbekendtgørelsen § 19** *Stk. 1.* 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.	Må ikke behandles elektronisk
Pseudonymiserede personfølsomme data	**Sikkerhedsbekendtgørelsen § 19** *Stk. 4.* Der skal foretages maskinel logning af bruger og tidspunkt for behandlingen	Identifikationsoplysninger skal krypteres eller erstattes af et kodenummer el. lign. Alternativt kan alle oplysninger lagres krypteret. Krypteringsnøgle, kodenøgle m.v. skal opbevares forsvarligt og adskilt fra personoplysningerne.

		Adgangen til projektdata må kun finde sted ved benyttelse af et fortroligt password. Password skal udskiftes mindst én gang om året, og når forholdene tilsiger det.
Fysiske vilkår	**Sikkerhedsbekendtgørelsen § 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 retningslinjer for myndighedens tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for myndigheden. **Sikkerhedsbekendtgørelsen § 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.	Lokaler, der benyttes til opbevaring og behandling af projektets oplysninger, skal være indrettet med henblik på at forhindre uvedkommende adgang. Behandling af oplysninger skal tilrettelægges således, at oplysningerne ikke hændeligt eller ulovligt tilintetgøres, fortabes eller forringes. Der skal endvidere foretages den fornødne kontrol for at sikre, at der ikke behandles urigtige eller vildledende oplysninger. Urigtige eller vildledende oplysninger eller oplysninger, som er behandlet i strid med loven eller disse vilkår, skal berigtiges eller slettes.
Biologisk materiale	*Biologisk materiale er ikke specifikt nævnt, men der kan henvises til persondatalovens § 41 stk. 3.* *Der skal, i virksomheden, laves retningslinjer der sikrer at denne overholdes.* *Rent praktisk skal disse retningslinjer ikke være ringere end dem, der gælder for privat forskning, hvorfor disse kan være et udgangspunkt for udformningen af de lokale regler.*	Prøver med biologisk materiale og biologisk materiale i biobanker skal opbevares forsvarligt aflåst, således at uvedkommende ikke har adgang til det, og på en sådan måde, at det sikres, at materialet ikke fortabes, forringes eller hændeligt eller ulovligt tilintetgøres. Biologisk materiale, der er mærket med personnummer eller navn, skal opbevares under iagttagelse af særlige sikkerhedshensyn. Der skal fastsættes interne retningslinjer i projektet for opbevaring af biologisk materiale. Retningslinjerne skal ajourføres mindst én gang om året.
Adgangsstyring	**Sikkerhedsbekendtgørelsen** § 11. Kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles. 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. Stk. 3. Der må endvidere autoriseres personer, for hvem adgang til oplysninger er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver. § 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. § 16. Autorisationer, jf. § 11, skal angive, i hvilket omfang brugeren må forespørge, inddatere eller slette personoplysninger. § 17. Det skal sikres, at de autoriserede personer fortsat opfylder betingelserne i § 11, stk. 2 og 3, og § 16.	Behandling af personoplysninger må kun foretages af den dataansvarlige eller på foranledning af den dataansvarlige og på dennes ansvar.

	Stk. 2. Kontrol heraf skal foretages mindst en gang hvert halve år.	
Sletning	**Persondatalovens § 5:** Stk. 5. Indsamlede oplysninger må ikke opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles. **Sikkerhedsbekendtgørelsen § 10.** 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. Stk. 3. Ved tilintetgørelse af inddatamateriale skal der træffes de fornødne sikkerhedsforanstaltninger mod, at materialet misbruges eller kommer til uvedkommendes kendskab. Der kan være tilfælde hvor det er relevant at overveje følgende: **Persondataloven § 41** 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.	Senest ved projektets afslutning skal oplysningerne slettes, anonymiseres eller tilintetgøres, således at det efterfølgende ikke er muligt at identificere enkeltpersoner, der indgår i undersøgelsen. Alternativt kan oplysningerne overføres til videre opbevaring i Statens Arkiver (herunder Dansk Dataarkiv) efter arkivlovens regler. Sletning af oplysninger fra elektroniske medier skal ske på en sådan måde, at oplysningerne ikke kan genetableres.
Databehandler	**Persondataloven § 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.	Datatilsynets vilkår gælder også ved behandling hos databehandler. Ved behandling hos databehandler skal der indgås en skriftlig aftale herom mellem den dataansvarlige og databehandleren. Det skal fremgå af aftalen, at databehandleren alene handler efter instruks fra den dataansvarlige, og at oplysninger ikke må anvendes til databehandlerens egne formål. Databehandleren skal desuden give den dataansvarlige tilstrækkelige oplysninger til, at denne til enhver tid kan sikre sig, at Datatilsynets vilkår kan overholdes, og at de bliver overholdt. Hvis databehandleren er etableret i en anden medlemsstat, skal det desuden fremgå af aftalen, at de yderligere bestemmelser om sikkerhedsforanstaltninger for databehandlere, som eventuelt er fastsat i den medlemsstat, hvor databehandleren er etableret, også er gældende for databehandleren.
Overførsel af oplysninger til tredjelande	Persondataloven § 27. Der må kun overføres oplysninger til et tredjeland, såfremt dette land sikrer et tilstrækkeligt beskyttelsesniveau, jf. dog stk. 3. Stk. 2. Vurderingen af, om beskyttelsesniveauet i et tredjeland er tilstrækkeligt, sker på grundlag af samtlige de forhold, der har indflydelse på en overførsel, herunder navnlig oplysningernes art, behandlingens formål og va-	• Overførsel af oplysninger til tredjelande, herunder til behandling hos databehandler samt til intern anvendelse i projektet, kræver forudgående tilladelse fra Datatilsynet. • Overførsel kan dog ske uden tilladelse, hvis den registrerede har givet udtrykkeligt samtykke til dette. Den registrerede

	righed, oprindelseslandet og det endelige bestemmelsesland, samt de retsregler, regler for god forretningsskik og sikkerhedsforanstaltninger, som gælder i tredjelandet. Stk. 3. Ud over de i stk. 1 nævnte tilfælde kan der overføres oplysninger til et tredjeland, såfremt 1) den registrerede har givet udtrykkeligt samtykke, 2) overførsel er nødvendig af hensyn til opfyldelsen af en aftale mellem den registrerede og den dataansvarlige eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en sådan aftale, 3) overførsel er nødvendig af hensyn til indgåelsen eller udførelsen af en aftale, der i den registreredes interesse er indgået mellem den dataansvarlige og tredjemand, 4) overførsel er nødvendig eller følger af lov eller bestemmelser fastsat i henhold til lov for at beskytte en vigtig samfundsmæssig interesse eller for, at et retskrav kan fastlægges, gøres gældende eller forsvares, 5) overførsel er nødvendig for at beskytte den registreredes vitale interesser, 6) overførsel finder sted fra et register, der ifølge lov eller bestemmelser fastsat i henhold til lov er tilgængeligt for offentligheden eller for personer, der kan godtgøre at have en berettiget interesse heri, i det omfang de i lovgivningen fastsatte betingelser for offentlig tilgængelighed er opfyldt i det specifikke tilfælde, 7) overførsel er nødvendig af hensyn til forebyggelse, efterforskning og forfølgning af strafbare forhold samt straffuldbyrdelse og beskyttelse af sigtede, vidner eller andre i sager om strafferetlig forfølgning eller 8) overførsel er nødvendig af hensyn til den offentlige sikkerhed, rigets forsvar eller statens sikkerhed. Stk. 4. Uden for de i stk. 3 nævnte tilfælde kan tilsynsmyndigheden give tilladelse til, at der overføres oplysninger til tredjelande, som ikke opfylder stk. 1, såfremt den dataansvarlige yder tilstrækkelige garantier for beskyttelse af de registreredes rettigheder. Der kan fastsættes nærmere vilkår for overførslen. Tilsynsmyndigheden underretter Europa-Kommissionen og de øvrige medlemsstater om tilladelser meddelt i henhold til denne bestemmelse. Stk. 5. Reglerne i denne lov finder i øvrigt anvendelse ved overførsel af oplysninger til tredjelande efter stk. 1, 3 og 4.	kan tilbagekalde samtykket. • Overførsel af oplysninger skal ske med bud eller anbefalet post. Ved elektronisk overførsel skal der træffes de fornødne sikkerhedsforanstaltninger mod, at oplysningerne kommer til uvedkommendes kendskab. Oplysningerne skal som minimum være forsvarligt krypteret under hele transmissionen. Datatilsynet fastsætter konkrete vilkår for overførsel ved hver tilladelse.

NOTAT

DANSKE REGIONER

Bilag 3

26-10-2010

Sag nr. 09/2825

It-understøttelse

Elektronisk behandling af data ved offentlig sundhedsforskning

Der gælder forskellige krav til den elektroniske behandling af data, afhængig af om data er pseudonymiserede eller ej.

Nedenfor gennemgås kravene til elektronisk behandling af data hhv. når data er pseudonymiserede, og når de ikke er det. Disse krav er ikke nye, men derimod en præcisering af allerede eksisterende krav til elektronisk behandling af data ved offentlig sundhedsforskning.

Offentlig forskning på pseudonymiserede data
For så vidt angår logningskravene til databehandlingen, skal der ved offentlig pseudonymiseret forskning finde maskinel logning af navn og tidspunkt sted.

Dette betyder rent it-mæssigt, at det er nok at foretage en form for maskinel logning af, hvilke personer der har haft adgang til data, og hvornår. Der skal ikke logges, hvad forskeren foretager sig med sine data.

Denne type forskning stiller således ikke voldsomme krav til it-understøttelsen af forskerens arbejdsgange. Scenariet for denne løsning er, at forskeren arbejder med sine data, der ligger på en fil-server, som maskinelt logger *hvem* der har haft adgang til data, og *hvornår* det er sket. De data der ligger på fil-serveren er pseudonymiserede, og nøglen er forsvarligt adskilt fra data.

Offentlig forskning på ikke-pseudonymiserede data
Logningskravene til offentlig forskning på ikke-pseudonymiserede data er mere vidtgående. Der skal således finde transaktionslogning sted, hvilket

betyder, at det maskinelt både skal logges *hvem* der har haft adgang til data, *hvornår* de har haft det, og *hvad* de har foretaget sig med data.

Denne type forskning stiller betydeligt større krav til it-understøttelsen af forskerens arbejdsgange. Scenariet for denne løsning er, at forskeren arbejder med sine data, der ligger på en database, som dels maskinelt logger hvem der har haft adgang til data hvornår, og dels hvad vedkommende har foretaget sig i arbejdet med data. Denne løsning er således væsentlig mere teknisk avanceret end den første løsning.

Ved begge løsninger henvises der til regionernes retningslinjer for arbejde med fortrolige data. Specifikt stiller Datatilsynet krav om, at hvis der sendes personhenførbare oplysninger over ubeskyttede net, herunder Internettet, skal data være krypteret med en stærk kryptering.