



Holbergsgade 6
DK-1057 København K

T +45 7226 9000
F +45 7226 9001
M sum@sum.dk
W sum.dk

Folketingets Sundheds- og Ældreudvalg

Dato: 04-11-2016
Enhed: Sundhedsøkonomi
Sagsbeh.: DEPSH
Sagsnr.: 1607575
Dok. nr.: 190610

Folketingets Sundheds- og Ældreudvalg har den 27. juli 2016 stillet følgende spørgsmål nr. 769 (Alm. del) til sundheds- og ældreministeren.

Spørgsmål nr. 769:

”Finder ministeren det tilfredsstillende, at SSI ved ikke at sikre en kryptering af data, dermed ikke har overholdt Datatilsynets anbefaling i udtalelse af 17. juni 2013 til SSI i forbindelse med en inspektion (Datatilsynet j.nr. 2012-621-0004), hvoraf det fremgår: ”Datatilsynet er bekendt med, at USB-pinde med persondata er bortkommet i forbindelse med almindelig postforsendelse. Henset til at der er tale om følsomme personoplysninger, og at der kan være tale om store datamængder omfattende mange borgere, vil tilsynet generelt anbefale, at sådanne data krypteres under forsendelse af lagringsmedier.”?

Spørgsmålet bedes være besvaret senest 2 dage inden ministerens besvarelse af SUU alm. del - samrådsspørgsmål AW og AX.”

Opfølgning på svar:

. / . Som opfølgning på besvarelse af SUU alm. del - spørgsmål 769, der blev afgivet den 6. september 2016, oversender jeg hermed Datatilsynets udtalelse af den 21. september på Sundheds- og Ældreministeriets henvendelse af den 18. august.

Som svar på spørgsmål 769 fremgår det, at Datatilsynets anbefalinger i udtalelse af 17. juni 2013 til SSI i forbindelse med en inspektion (Datatilsynet j.nr. 2012-621-0004) ikke blev fulgt jf. Datatilsynets vurdering i medfølgende udtalelse.

Af Sundhedsdatastyrelsens ”Redegørelse om fejlaflevering af anbefalet brev indeholdende personoplysninger” af den 1. september fremgår, det at:

”Da den fejlliveredede dataleverance fulgte den gældende politik i Forskerservice, undersøgte Statens Serum Institut baggrunden for den risikovurdering, der lå til grund for ikke at kryptere forsendelser. I 2013 anbefalede Datatilsynet – på baggrund af en inspektion af Sundhedsstyrelsen i 2011 – Statens Serum Institut, at datamedier krypteres ved forsendelse med almindelig postforsendelse. Statens Serum Institut hæftede sig dengang ved, at Datatilsynets anbefaling henviste til spørgsmålet om, hvorvidt almindelig post var tilstrækkelig, hvorimod Statens Serum Institut anvendte rekommanderet post. Det var Statens Serum Instituts vurdering, at risikoen for ødelæggelse, bortkomst, tyveri eller fejlaflevering var væsentligt lavere ved rekommanderet post end ved almindelig post.”

Informationssikkerhed er helt afgørende for anvendelsen af helbredsoplysninger i det danske sundhedsvæsen. Med Datatilsynets udtalelse er jeg blevet bekræftet i vigtig-

heden af, at der er styr på procedurerne og arbejdsgangene omkring håndteringen af personfølsomme oplysninger. Det er ikke tilfredsstillende, når der er tvivl om anbefalingerne fra de tilsynsførende myndigheder, og når disse ikke bliver fulgt. Jeg er også blevet bekræftet i, at det var relevant at igangsætte serviceeftersynet i Sundheds- og Ældreministeriets concern af blandt andet håndteringen af følsomme personoplysninger ift. gældende sikkerhedskrav og generelt inden for lovgivningens rammer.

Datatilsynets udtalelse oversendes til Sundhedsdatastyrelsen under Sundheds- og Ældreministeriet. Jeg forventer at kunne oplyse jer nærmere om styrelsens uddybende kommentarer hertil ved det kommende samråd om sagen, der er berammet til den 1. december 2016. De øvrige styrelser orienteres ligeledes om Datatilsynets udtalelse.

Jeg vil som lovet løbende holde udvalget orienteret om det videre forløb med serviceeftersynet.

Med venlig hilsen

Sophie Løhde / Sandra Poulsen

Folketingets Sundheds- og Ældreudvalg

Dato: 06-09-2016
Enhed: Sundhedsøkonomi
Sagsbeh.: DEPSHP
Sagsnr.: 1607575
Dok. nr.: 151338

Folketingets Sundheds- og Ældreudvalg har den 27. juli 2016 stillet følgende spørgsmål nr. 769 (Alm. del) til sundheds- og ældreministeren, som hermed besvares. Spørgsmålet er stillet efter ønske fra Peder Hvelplund (EL).

Spørgsmål nr. 769:

”Finder ministeren det tilfredsstillende, at SSI ved ikke at sikre en kryptering af data, dermed ikke har overholdt Datatilsynets anbefaling i udtalelse af 17. juni 2013 til SSI i forbindelse med en inspektion (Datatilsynet j.nr. 2012-621-0004), hvoraf det fremgår: ”Datatilsynet er bekendt med, at USB-pinde med persondata er bortkommet i forbindelse med almindelig postforsendelse. Henset til at der er tale om følsomme personoplysninger, og at der kan være tale om store datamængder omfattende mange borgere, vil tilsynet generelt anbefale, at sådanne data krypteres under forsendelse af lagringsmedier.”?

Spørgsmålet bedes være besvaret senest 2 dage inden ministerens besvarelse af SUU alm. del - samrådsspørgsmål AW og AX.”

Svar:

Mit ministerium har bedt Datatilsynet oplyse om, hvorvidt Statens Serum Institut, ved ikke at sikre en kryptering af data på datamedierne (to CD'er), dermed ikke har overholdt Datatilsynets anbefaling i udtalelse af 17. juni 2013 til SSI i forbindelse med en inspektion. (Datatilsynet j.nr. 2012-621-0004).

Endvidere er Datatilsynet blevet udbedt at oplyse om, til hvilke bortkomne lagringsmedier, der henvises til i Datatilsynets udtalelse i forbindelse med ovennævnte inspektion af Statens Serum Institut.

Det fremgår af den til SUU 766 vedlagte redegørelse, at Statens Serum Institut som følge af hændelsen i februar 2015, ændrede praksis.

Med venlig hilsen

Sophie Løhde / Sandra Poulsen

Folketingets Sundheds- og Ældreudvalg

Dato: 06-09-2016
Enhed: Sundhedsøkonomi
Sagsbeh.: DEPSHP
Sagsnr.: 1607575
Dok. nr.: 151323

Folketingets Sundheds- og Ældreudvalg har den 27. juli 2016 stillet følgende spørgsmål nr. 766 (Alm. del) til sundheds- og ældreministeren, som hermed besvares. Spørgsmålet er stillet efter ønske fra Peder Hvelplund (EL).

Spørgsmål nr. 766:

”Mener ministeren, at det er tilfredsstillende, at der går 17 måneder, før lækagen af 5,28 mio. CPR-nr. til Chines Visa Application Center kommer til offentlighedens kendskab, og i forlængelse heraf bedes ministeren svare på, hvornår ministeren fik kendskab til lækagen?”

Spørgsmålet bedes være besvaret senest 2 dage inden ministerens besvarelse af SUU alm. del - samrådsspørgsmål AW og AX.”

Svar:

Jeg ser med stor alvor på denne sag og på datasikkerhed i sundhedsvæsenet. Jeg blev derfor både overrasket og meget ærgerlig over sagen, da den kom til mit kendskab den 20. juli i forbindelse med omtalen i pressen. Jeg fik således først kendskab til sagen samtidig med offentligheden.

Som jeg netop også har orienteret udvalget om, er det kommet til mit kendskab, at der er to andre sager om videregivelse af personfølsomme oplysninger, der er kommet uvedkommende i hænde. Det giver mig anledning til at sætte et arbejde i gang, så vi fremadrettet minimerer risikoen for, at noget lignende kan ske igen. Jeg vil derfor med inddragelse af eksterne konsulenter iværksætte et serviceeftersyn af hele Sundheds- og Ældreministeriets koncern. Det skal blandt andet sikre, at styrelserne håndterer personfølsomme oplysninger korrekt i alle arbejdsgange, så de ikke udleveres til uvedkommende.

Det er utroligt vigtigt, at vi gør alt, hvad vi kan for at minimere risikoen for at personoplysninger, som vi har ansvaret for, kommer uvedkommende i hænde. Det er på den baggrund, at jeg nu iværksætter serviceeftersynet.

Datasikkerhed er helt afgørende, når man gerne vil anvende data til at gøre sundhedsvæsenet bedre.

. / . Med hensyn til den konkrete sag, der omtales i spørgsmålet, har mit ministerium bedt Sundhedsdatastyrelsen om en redegørelse, som er vedlagt denne besvarelse.

Jeg kan desuden oplyse, at det daværende ministerium – Ministeriet for Sundhed og Forebyggelse – blev orienteret om sagen af Statens Serum Institut samt om instituttets håndtering heraf den 23. februar 2015, herunder at Datatilsynet, den tilsynsførende myndighed, var blevet kontaktet med henblik på at foretage relevant opfølgning på sagen.

Jeg mener generelt, at åbenhed er helt afgørende, og at sagens fakta skal frem. Jeg vil derfor bede Sundhedsdatastyrelsen om at fremlægge den vedhæftede redegørelse på deres hjemmeside, således at den også er tilgængelig for offentligheden der.

Jeg kan i øvrigt henvise til min besvarelse af SUU 767.

Med venlig hilsen

Sophie Løhde / Sandra Poulsen

Til Sundheds- og Ældreministeriet

Redegørelse om fejlaflevering af anbefalet brev indeholdende personoplysninger.

Sundhedsdatastyrelsen er blevet bedt om en redegørelse for sagen vedrørende et fejlafleveret anbefalet brev indeholdende persondata. Brevet blev afsendt fra Statens Serum Instituts Forskerservice. Brevet var adresseret til Danmarks Statistik, men blev i februar 2015 afleveret af Post Danmark til Chinese Visa Application Centre, en privat virksomhed der formidler visumansøgninger til Kina.

Redegørelsen skal bl.a. indeholde følgende:

- A. Beskrivelse af sagsforløbet (kronologisk fremstilling)
- B. Information om baggrunden for SSI's fremsendelse af personnumre og helbredsoplysninger til Danmarks Statistik
- C. Redegørelse om, hvilke tiltag Sundhedsdatastyrelsen har taget som led i håndteringen af sagen og i øvrigt med henblik på at sikre en mere professionel sagsbehandlingspraksis
- D. Information om, hvorledes sagsbehandlingen og udlevering af data foregår i dag (til Danmarks Statistik såvel som til andre)

Nedenfor følger Sundhedsdatastyrelsens redegørelse for den konkrete sag.

Sundhedsdatastyrelsen udarbejder redegørelsen, da Forskerservice blev overført fra Statens Serum Institut til Sundhedsdatastyrelsen ved etableringen af Sundhedsdatastyrelsen i november 2015. Indtil 2012 var Forskerservice en del af Sundhedsstyrelsen.

Redegørelse

Sundhedsdatastyrelsen skal indledningsvis beklage, at personfølsomme data blev fremsendt ukrypteret til Danmarks Statistik og dermed potentielt kunne være kommet til uvedkommendes kendskab. Der var tale om en utilstrækkelig praksis, som burde have været ændret før denne hændelse.

A. Beskrivelse af sagsforløbet

I den konkrete sag fra februar 2015 skulle en forsker fra Statens Institut for Folkesundhed efter aftale med Sundhedsstyrelsen koble data fra en række datakilder, herunder sundhedsregistre, på en Forskermaskine hos Danmarks Statistik til brug for forskningsprojektet "Sygdomsbyrden i Danmark – udvalgte risikofaktorer og sygdomme med fokus på social ulighed"¹. Forskningsprojektet skulle gennemføres på Danmarks Statistiks forskermaskiner, hvor forskeren har adgang til pseudonymiserede data til brug for projektet.

Efter at have behandlet forskerens ansøgning, sendte Forskerservice på Statens Serum Institut derfor et datasæt indeholdende CPR-numre og helbredsdata til Danmarks Statistik. I forbindelse med modtagelsen hos Danmarks Statistik skulle datasættet pseudonymiseres af Danmarks Statistik.

Forskerservice kunne ikke pseudonymisere data på forhånd, da alle data forskeren skulle have adgang til, dvs. også data fra andre end Statens Serum Institut, skulle være krypteret efter samme nøgle hos Danmarks Statistik.

Den 16. februar 2015 afsendte Forskerservice på Statens Serum Institut derfor et rekommanderet brev adresseret til Danmarks Statistik, Sejrøgade 11, 2100 København Ø. Brevet indeholdt et følgebrev samt to CD'er med data til brug for ovennævnte projekt. Jf. den daværende praksis var CD'erne ikke krypterede.

De to CD'er indeholdt CPR-data om 5.282.616 personer bosat i danske kommuner mellem 2010 og 2012. CD'erne indeholdt CPR-numre for personer, der opfyldte bestemte bopælskriterier, men ikke navn og adresse. For så vidt angår ca. 1.150.300 borgere indeholdt datasættet endvidere helbredsoplysninger fra cancerregisteret, diabetesregisteret og/eller det centrale psykiatriske register.

Den 17. og 18. februar 2015 blev Statens Serum Institut kontaktet henholdsvis telefonisk og skriftligt af Danmarks Statistik, der havde fået overbragt brevet fra en medarbejder på Chinese Visa Application Centre, som fejlagtigt havde modtaget - og åbnet - brevet. Chinese Visa Application Centre er beliggende på Lyngbyvej 28, 2100 København Ø og er en dansk registreret virksomhed med kinesiske ejere, der bistår privatpersoner med at indhente visum til Kina.

¹ https://sundhedsstyrelsen.dk/da/sygdom-og-behandling/~/_/media/00C6825B11BD46F9B064536C6E7DFBA0.ashx

Statens Serum Institut tog kontakt til Chinese Visa Application Centre, der imidlertid var ferielukket, hvilket den 23. februar 2015 blev fulgt op at et besøg hos virksomheden, hvor ledende medarbejdere fra Statens Serum Institut modtog en mundtlig redegørelse for forløbet. Statens Serum Institut orienterede herefter Datatilsynet telefonisk og skriftligt om hændelsen.

Medarbejderen fra Chinese Visa Application Centre, der havde modtaget brevet, oplyste ved denne lejlighed, at det først var efter åbningen, at hun konstaterede, at brevet var fejlafleveret. Hun gik derefter straks de 250 m. til Danmarks Statistik, hvor hun afleverede brevet i receptionen.

Statens Serum institut modtog den 4. marts 2015 en skriftlig bekræftelse på dette sagsforløb og har ikke fundet grund til at betvivle forklaringen. Som sagen er oplyst er der således ikke tale om, at data er "lækket", men alene at forsendelseskæden har været brudt, men ikke kompromitteret.

Forskerservice kontaktede endvidere den 3. marts 2015 Post Danmark (nu: Post Nord) med henblik på at få oplyst, hvordan en sådan fejlaflevering kunne ske, samt hvad de ville gøre for, at undgå tilsvarende hændelser opstod igen. Efter gentagne rykkestilfælde har Post Nord i september 2015 oplyst, at der var tale om en menneskelig fejl, at det ikke er muligt nærmere at forklare fejlen, da den pågældende medarbejder er fratrukket, og at man på det pågældende omdelingskontor har indskærpet vigtigheden af, at (rekommanderede) breve afleveres til rette modtager.

Da den fejlleverede dataleverance fulgte den gældende politik i Forskerservice, undersøgte Statens Serum Institut baggrunden for den risikovurdering, der lå til grund for ikke at kryptere forsendelser. I 2013 anbefalede Datatilsynet – på baggrund af en inspektion af Sundhedsstyrelsen i 2011 – Statens Serum Institut, at datamedier krypteres ved forsendelse med almindelig postforsendelse. Statens Serum Institut hæftede sig dengang ved, at Datatilsynets anbefaling henviste til spørgsmålet om, hvorvidt almindelig post var tilstrækkelig, hvorimod Statens Serum Institut anvendte rekommanderet post. Det var Statens Serum Instituts vurdering, at risikoen for ødelæggelse, bortkomst, tyveri eller fejlaflevering var væsentligt lavere ved rekommanderet post end ved almindelig post.

Som følge af hændelsen i februar 2015 foretog Statens Serum institut en fornyet risikovurdering og introducerede kryptering uanset om data fremsendes med almindelig eller rekommanderet post. I praksis sender Forskerservice dog aldrig personhenførbare helbredsoplysninger med almindelig post. Derudover blev udveksling af data med Danmarks Statistik ændret fra rekommanderet post til en direkte dataforbindelse.

Da der efter Statens Serum Instituts vurdering ikke var tale om, at data var kompromitteret, fandt man ikke grundlag for at orientere de potentielt berørte borgere, jf. nedenstående dialog med Datatilsynet om sagen.

Dialogen med Datatilsynet og Datatilsynets udtalelse af 15. juli 2016

I sin henvendelse til Datatilsynet i februar 2015 redegjorde Statens Serum Institut for sagens forløb, herunder at der ikke efter deres vurdering var tale om, at data var kompromitteret. Forskerservice oplyste, at der derfor ikke var grundlag for at orientere de potentielt berørte borgere om hændelsen.

Datatilsynet udbad sig på baggrund af sagen en række supplerende oplysninger, herunder sagens forløb, oplysning om Post Danmarks (nu: Post Nords) udtalelse om sagen og om tiltag og ændret praksis i Forskerservice på baggrund af sagen.

Datatilsynet har i sin udtalelse af 15. juli 2016 noteret sig det oplyste om, at Statens Serum Institut foranlediget af den konkrete henvendelse ændrede sine retningslinjer for fremsendelse af datamedier i breve, således at data fremover altid skal krypteres.

Datatilsynet udtaler således ikke i sin afgørelse bagudrettet kritik af den manglende kryptering, ligesom Datatilsynet efter sin sagsbehandling ikke påtaler en tilsidesættelse af persondatalovens regler.

Datatilsynet har endvidere noteret sig det oplyste om Statens Serum Instituts overvejelser og kan efter omstændighederne tiltræde konklusionen om ikke at fremsende individuel information til de berørte personer.

B. Information om baggrunden for Statens Serum Instituts fremsendelse af personnumre og helbredsoplysninger til Danmarks Statistik

Forskerservice under Sundhedsdatastyrelsen (tidligere under Statens Serum Institut) har til opgave at understøtte registerforskningen i Danmark på sundhedsområdet. Forskere, der har brug for data i forbindelse med forskning, kan via Forskerservice ansøge om registerdata på sundhedsområdet.

Forskerservice er endvidere databehandler for Social- og Indenrigsministeriet og leverer udtræk fra CPR-registeret til forskere på vegne af Social- og Indenrigsministeriet.

Forskerservice kan efter en konkret vurdering af ansøgningen give adgang til sundhedsdata på to måder: Enten som dataudtræk sendt til forskeren (enten direkte eller til indlæsning på forskermaskiner hos Danmarks Statistik) eller via Sundhedsdatastyrelsens Forskermaskiner, hvor forskeren arbejder med pseudonymiserede data hos Sundhedsdatastyrelsen.

Forsendelse af data til forskere er især relevant, hvor forskere enten har behov for at koble data fra Sundhedsdatastyrelsen med andre data, fx uddannelsesmæssige eller beskæftigelsesmæssige oplysninger, eller har behov for adgang til konkrete lægejournaler, laboratorieresultater eller lignende.

Hjemlen til at videregive data til forskningsformål følger af persondatalovens § 10, hvorefter personfølsomme data, jf. lovens §§ 7 og 8, kan anvendes til at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning.

Lovens § 6, stk. 1, nr. 5, giver endvidere adgang til at behandle såkaldte almindelige, ikke-følsomme oplysninger, hvis behandlingen er nødvendig af hensynet til udførelsen af en opgave i samfundets interesse. Omfattet heraf er forsknings- og statistikformål.

I medfør af § 11, stk. 1, kan offentlige myndigheder behandle oplysninger om personnummer (CPR-nummer) med henblik på en entydig identifikation mv., herunder i forbindelse med forsknings- og statistikformål. I medfør af § 11, stk. 2, nr. 3, kan private også behandle personnumre, hvis behandlingen alene finder sted til videnskabelige eller statistiske formål.

Håndteringen af personoplysninger skal leve op til kravet om fornødne sikkerhedsforanstaltninger i persondatalovens § 41, stk. 3, hvorefter 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.

Det fremgår af forarbejderne til bestemmelsen, at det forudsættes, at foranstaltningerne under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse, vil tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, som skal beskyttes, jf. persondatadirektivets artikel 17, stk. 1, 2. afsnit.

C. Redegørelse om, hvilke tiltag Sundhedsdatastyrelsen har taget som led i håndteringen af sagen og i øvrigt med henblik på at sikre en mere professionel sagsbehandlingspraksis

Umiddelbart efter hændelsen ændrede Forskerservice/Statens Serum Institut praksis på to konkrete områder:

- Der blev indført kryptering på alle forsendelser indeholdende CPR-numre, uanset om fremsendelsesbrevet er med almindeligt eller rekommanderet post. I praksis sender Forskerservice dog aldrig personhenførbare helbredsoplysninger med almindelig post.
- Kommunikationen med Danmarks Statistik er omlagt, således at kommunikation nu sker uden brug af postvæsenet, men via en direkte, lukket og krypteret dataforbindelse.

Etableringen af Sundhedsdatastyrelsen har blandt andet haft til hensigt at øge fokus på informationssikkerhed. Styrelsen har derfor generelt gennemgået processer og procedurer og skærpet sikkerhedsniveauet. Derudover har styrelsen etableret en dedikeret afdeling for Compliance og Informationssikkerhed, der har juridisk og teknisk ekspertise på området, bistår med risikovurderinger, stiller krav til sikkerhedsforanstaltninger op på efterlevelsen af disse, bistået af ekstern konsulentbistand hvor relevant.

Som bekendt pågår der i forbindelse med Forskerservice arbejde med at reducere antallet af dataforsendelser og i stedet give adgang til pseudonymiserede sundhedsdata på de såkaldte Forskermaskiner. En øget brug af Forskermaskiner vil yderligere styrke procedurerne omkring videregivelse af helbredsoplysninger. Det vil dog fortsat være nødvendigt at videregive data i en række situationer, herunder når data skal kobles med andre data på Danmarks Statistiks Forskermaskiner.

Arbejdet med ibrugtagning af Forskermaskiner, hvor data ikke forlader Sundhedsdatastyrelsens tekniske miljø, er efter sagen intensiveret med henblik på at nedbringe antallet af dataforsendelser.

Det bemærkes, at uanset forskermaskiner hos Sundhedsdatastyrelsen vil det fortsat være nødvendigt at sende data indeholdende CPR-numre til Danmarks Statistik, da Danmarks Statistik ikke tillader, at mikrodata (data på individniveau) fra Danmarks Statistiks registre forlader Danmarks Statistik.

I de tilfælde, hvor en forsker skal koble data fra Danmarks Statistik og Sundhedsdatastyrelsen, vil data således skulle transporteres fra Sundhedsdatastyrelsen til Danmarks Statistik via en direkte, lukket og krypteret dataforbindelse – uanset fordelingen i tyngde eller følsomhed i data fra hhv. Sundhedsdatastyrelsen og Danmarks Statistik.

D. Information om, hvorledes sagsbehandlingen og udlevering af data foregår i dag

Sagsbehandlingen i Forskerservice foregår i dag således:

- Forskerservice modtager en ansøgning om dataudtræk eller adgang via Forskermaskinen
- Forskerservice kontrollerer, at de formelle kriterier for ansøgningen er opfyldt: at databehandlingen som led i projektet er anmeldt til Datatilsynet, som har afgivet udtalelse², at der er dansk dataansvarlig, og at projektet er af væsentlig samfundsmæssig betydning mv.
- Forskerservice går i dialog med forskeren omkring indholdet af dataudtræk for at sikre, at der er den fornødne proportionalitet imellem forskningsprojektets genstandsfelt og det ønskede dataudtræk,
- Hvis forskeren ansøger om at modtage data med CPR-numre (fremfor pseudonymiserede data) skal dette være begrundet og nødvendigt i forhold til forskningsprojektet
- Data stilles til rådighed for forskeren enten
 - o på Sundhedsdatastyrelsens Forskermaskiner, eller
 - o på Danmarks Statistiks Forskermaskiner (i så fald sendes CPR-nummer baserede data via sikker FTP til Danmarks Statistik), eller
 - o ved at data sendes på krypteret USB-stik med anbefalet post til forskeren (uanset om data indeholder CPR-numre eller er pseudonymiserede).

² Eller meddelt tilladelse, hvis den dataansvarlige forsker er privat.



Sundheds- og Ældreministeriet
Holbergsgade 6
1057 København K

Sendt til: SSHP@sum.dk

21. september 2016

Vedrørende Sundheds- og Ældreministeriets forespørgsel af 18. august 2016

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

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

J.nr. 2016-321-0425
Sagsbehandler
Anders Petersen
Direkte 3319 3221

Ved e-mail af 18. august 2016 har Sundheds- og Ældreministeriet rettet henvendelse til Datatilsynet vedrørende sagen om et anbefalet brev, der blev afleveret til en forkert modtager.

1. Sundheds- og Ældreministeriet har anmodet Datatilsynet om at oplyse, om Statens Serum Institut ved ikke at sikre en kryptering af datamedierne (to CD'er), dermed ikke har overholdt Datatilsynets anbefaling i udtalelse af 17. juni 2013 til SSI i forbindelse med en inspektion.

I forbindelse med Datatilsynets inspektion i 2011 stillede SSI tilsynet et spørgsmål om fremsendelse af datamedier med almindelig post. Datatilsynet svarede, at tilsynet vil anbefale, at data krypteres under forsendelse af lagringsmedier.

I sagen, hvor to CD'er i 2015 blev afleveret til en forkert modtager, havde SSI ikke krypteret dataene og havde således ikke fulgt Datatilsynets anbefaling.

2. Det kan uddybende oplyses, at persondatalovens¹ sikkerhedskrav² indebærer, at de dataansvarlige myndigheder, virksomheder mv. skal beskytte personoplysninger med de fornødne sikkerhedsforanstaltninger. Dette gælder f.eks., når personoplysningerne overføres til diverse former for datamedier og –udstyr, hvor oplysningerne lagres og opbevares.

Persondatalovens krav om datasikkerhed medfører således, at personoplysninger, der behandles på bærbare datamedier mv., skal beskyttes ikke blot under forsendelse, men også når datamedierne mv. opbevares hos afsender og modtager.

Det kan tilføjes, at Datatilsynet i visse tilfælde har stillet egentlige krav til lagringen af følsomme personoplysninger i form af vilkår. Ved behandling af

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

² Af persondatalovens § 41, stk. 3, fremgår, at der skal træffes 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..

følsomme personoplysninger i privat forskning indeholder Datatilsynets standardvilkår således bl.a. følgende:

”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.”

Datatilsynet har i sikkerhedsvejledningen³ endvidere angivet, at personoplysninger, der lagres lokalt (uden for det centrale system), bør krypteres i forbindelse med hjemmearbejdspladser.

3. Sundheds- og Ældreministeriet har endvidere anmodet Datatilsynet om at oplyse, hvilke bortkomne lagringsmedier der henvises til i Datatilsynets udtalelse af 17. juni 2013.

Det kan i den forbindelse oplyses, at Datatilsynet i mindst to tilfælde er blevet orienteret af dataansvarlige myndigheder eller virksomheder om, at USB-nøgler med persondata er bortkommet i forbindelse med almindelig postforsendelse. Disse henvendelser har ikke omhandlet forskningsdata eller i øvrigt data fra SSI.

4. Det kan tilføjes, at tilsynet også har modtaget henvendelser, hvor lagringsmedier mv. er bortkommet hos den dataansvarlige, efter at forsendelsen har fundet sted; f.eks. hvor USB-nøgler efter modtagelsen er blevet opbevaret hos modtageren og derefter stjålet. Eksempler herpå har også været omtalt i medierne⁴. Dette understreger vigtigheden af, at persondatalovens krav om beskyttelse af personoplysninger på diverse former for datamedier altid iagttages.

Efter Datatilsynets opfattelse må lagring af fortrolige eller følsomme personoplysninger på bærbare datamedier samt pc'er og andet it-udstyr, der forholdsvis nemt kan bortkomme eller stjæles, give anledning til særlig opmærksomhed på beskyttelse af oplysningerne.

De dataansvarlige myndigheder og virksomheder mv. bør efter Datatilsynets opfattelse have retningslinjer for beskyttelse af personoplysninger på såvel bærbare datamedier som bærbare pc'er og andet it-udstyr. Afhængigt af omstændighederne vil kryptering eller pseudonymisering eventuelt være en nødvendig sikkerhedsforanstaltning.

Med venlig hilsen

Lena Andersen
Kontorchef

³ Datatilsynets vejledning nr. 37 af 2. april 2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning. Se vejledningen til § 7, stk. 2, vedrørende hjemmearbejdspladser.

⁴ Se f.eks. <http://politiken.dk/indland/ECE2387183/indbrudstyre-stjal-computer-og--usb-stik-fra-skattesagskommission/>