DATATILSYNET

Sundheds- og Ældreministeriet
Holbergsgade 6
1057 København K

Sendt til: SSHP@sum.dk

21. september 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

Vedrørende Sundheds- og Ældreministeriets forespørgsel af 18. august 2016

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 persondatalovens[1] sikkerhedskrav[2] 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 sikkerhedsvejledningen[3] 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 medierne[4]. 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 omstædighederne 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/indbrudstyve-stjal-computer-og--usb-stik-fra-skattesagskommission/