DATATILSYNET

Fredensborg Kommune
Egevangen 3B
2980 Kokkedal

Sendt til mtm@fredensborg.dk med kopi til
fredensborg@fredensborg.dk

14. februar 2017

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. 2017-323-0455
Dok.nr. 417998
Sagsbehandler
Cathrine E Sørensen
Direkte 3319 3229

Vedrørende kontrol af internettrafik og e-mails

Ved brev af 7. februar 2017 har Fredensborg Kommune rettet henvendelse til Datatilsynet vedrørende logning af internettrafik og e-mails.

Af henvendelsen fremgår bl.a., at Fredensborg Kommune overvejer at foretage kontrol af trafik på kommunens internet- og mailservere i forhold til såvel medarbejdere som bestyrelsesmedlemmer.

I den anledning afgiver Datatilsynet følgende vejledende udtalelse:

1. Anmeldelse til Datatilsynet
I medfør af persondataloven[1] har Fredensborg Kommune i 2008 foretaget anmeldelse[2] af behandlingen "Kontrol af medarbejdernes anvendelse af e-mail og internet".

Af anmeldelsen fremgår bl.a. under punkt 4, at der behandles oplysninger om medarbejdere, studerende og andre brugere, som har afgang til at anvende kommunens postsystem og internettet via kommunens internetforbindelser.

Datatilsynet har i den anledning afgivet udtalelse[3] til Fredensborg Kommune den 19. juni 2008. Datatilsynet havde ikke bemærkninger til anmeldelsen.

Efter Datatilsynets opfattelse må anmeldelsen med angivelsen "andre brugere" antages også at omfatte byrådsmedlemmer, når disse benytter kommunens internet- og mailserver som led i deres hverv.

2. Kontrol af brug af internet og e-mails
På Datatilsynets hjemmeside er gengivet en række udtalelser om kontrol af medarbejderes brug af internet og e-mail.[4]

[1] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer
[2] Datatilsynets j.nr. 2008-52-0051
[3] Jf. § 45
[4] Se bl.a. Datatilsynet j.nr. 2000-631-0001 og 2000-632-0001. Afgørelserne er tilgængelige på www.datatilsynet.dk under punktet "Publikationer"

Datatilsynet har noteret sig, at Fredensborg Kommune er bekendt med Datatilsynets praksis og antager, at tilsvarende regler vil være gældende for byrådsmedlemmernes datatrafik.

Datatilsynet kan bekræfte, at det er de samme regler i persondataloven, som finder anvendelse – uanset om de registrerede er ansatte eller byrådsmedlemmer. Det afgørende er imidlertid, om der i de konkrete tilfælde foreligger en nødvendig behandling, og om kommunens interesse i behandlingen overstiger hensynet til de berørte personer.

Persondataloven giver således mulighed for, at behandling kan finde sted, bl.a. hvis det er nødvendigt for, at Fredensborg Kommune kan forfølge berettigede interesser, og hensynet til de registrerede ikke overstiger disse interesser. Som eksempler på berettigede interesser kan nævntes tekniske og sikkerhedsmæssige hensyn, drift samt kontrol af at myndighedens retningslinjer overholdes.

Endvidere vil behandling kunne finde sted, hvis det i øvrigt er nødvendigt af hensyn til udførelsen af en opgave i samfundets interesse eller til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som den dataansvarlige eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt.

Det er i første række Fredensborg Kommune, der som dataansvarlig skal foretage en vurdering af, om de ønskede behandlinger kan og skal ske indenfor persondatalovens rammer.

3. Forudgående information

Datatilsynet har noteret sig, at Fredensborg Kommune er bekendt med, at det fremgår af Datatilsynets praksis[5], at det er en forudsætning, at de registrerede på forhånd er orienteret om logningen og den mulige brug heraf.

Som følge af princippet om god databehandlingsskik i persondatalovens § 5, stk. 1, forudsætter en arbejdsgivers kontrol af de ansattes e-mail således normalt, at de ansatte på forhånd på en klar og utvetydig måde er informeret om, at kontrol kan finde sted.

Datatilsynet bemærker, at det i Fredensborg Kommunes henvendelse er oplyst, at kommunen i sin IT-politik – som i øvrigt er blevet forelagt byrådsmedlemmerne ved deres tiltræden – informerer om, at al aktivitet på internettet og i e-postsystemer bliver logget.

Hvis der ikke tillige er givet klar og utvetydig forudgående information om, at brug af internet og e-mails kan blive gennemset som led i en kontrol ved mistanke om brug af internet eller e-mails i strid med arbejdspladsens retningslin-

[5] Se bl.a. Datatilsynets j.nr. 2002-219-0110. Afgørelsen er tilgængelig på www.datatilsynet.dk under punktet "Afgørelser"

jer, har Fredensborg Kommune efter Datatilsynets umiddelbare vurdering ikke givet en forudgående information.

Det bemærkes herved, at informationer, som er givet efter den episode, som overvejes undersøgt, efter Datatilsynets umiddelbare opfattelse ikke kan anses for "forudgående information" som forudsat i tilsynets praksis.

Fredensborg Kommune må i givet fald overveje, om der i de konkrete tilfælde er grundlag for, at kravet om forudgående information kan fraviges.

Datatilsynet har i en konkret sag[6] udtalt, at princippet om god databehandlingsskik efter tilsynets opfattelse medfører, at der i forbindelse med tv-overvågning i kontroløjemed som den absolutte hovedregel skal gives forudgående information til de ansatte. Ved vurderingen af, om der kan ske fravigelse af denne hovedregel, må de hensyn, der kan begrunde fravigelse af oplysningspligt, jf. § 30, jf. §§ 28 og 29, inddrages. Det vil sige, at der skal være tale om afgørende hensyn til private eller offentlige interesser.

Datatilsynet skal understrege, at den absolutte hovedregel er, at der forudgående skal være givet klar og utvetydig information om bl.a. muligheden for kontrol. Muligheden for undtagelsesvist at foretage kontrollen uden forudgående information er således underlagt ganske snævre grænser, jf. herved også henvisningen til § 30 i persondataloven.

Datatilsynet har i en konkret sag bl.a. fundet, at den omstændighed, at oplysningerne var blevet anvendt på baggrund af konkrete mistanker, ikke kunne bevirke, at der ikke skulle gives forudgående information om den mulige sammenstilling og brug af oplysningerne. De hensyn til de registrerede, som ligger bag kravet om forudgående information, gør sig således gældende, uanset om en behandling af oplysninger i kontroløjemed sker som stikprøvekontrol eller på baggrund af en konkret mistanke.

Det er også på dette punkt i første række Fredensborg Kommune, der som dataansvarlig skal foretage en vurdering af, om kravet om forudgående information kan og bør fraviges i de konkrete tilfælde. Datatilsynet vil kunne tage konkret stilling hertil efterfølgende, f.eks. i tilfælde en klage fra en af de berørte personer.

4. Logning efter sikkerhedsbekendtgørelsens § 19

Det fremgår ikke klart af henvendelsen fra Fredensborg Kommune, om der også er tale om at anvende en sikkerhedslog efter sikkerhedsbekendtgørelsens[7] § 19 (en "§ 19-log").

---

[6] Datatilsynets j.nr. 2002-219-0110. Afgørelsen er omtalt i Datatilsynets Årsberetning 2003, s. 99f., som er tilgængelig på www.datatilsynet.dk under punktet "Publikationer"

[7] Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000, som ændret ved bekendtgørelse nr. 201 af 22. marts 2001, om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

Efter Datatilsynets opfattelse må en "§ 19-log" bruges til at undersøge, om anvendelsen af personoplysninger har været i overensstemmelse med persondataloven. Når dette sker, er der efter tilsynets opfattelse tale om en del af den dataansvarliges efterlevelse af persondatalovens sikkerhedskrav.

Det er i den forbindelse tilsynets umiddelbare vurdering, at anvendelsen af en "§ 19-log" til kontrol inden for rammerne af persondatalovens § 41, stk. 3, er en sikkerhedsforanstaltning, og derfor ikke tillige skal have en selvstændig behandlingshjemmel i persondatalovens kapitel 4.

Det er i første række den enkelte myndighed, der må vurdere og beslutte, hvilke sikkerhedsforanstaltninger der er nødvendige i en given situation. Herunder om der skal ske kontrol af loggen.

Datatilsynet har på enkelte områder (bl.a. i forhold til kommunernes borgerservicecentre) stillet krav om regelmæssig stikprøvekontrol ved brug af loggen. Dette udelukker imidlertid ikke, at stikprøvekontrol kan være en del af de fornødne sikkerhedsforanstaltninger på andre områder.

Ved mistanke om misbrug af adgang til personoplysninger er det endvidere Datatilsynets opfattelse, at myndigheden må og skal undersøge dette. En myndighed, der ignorerer en mistanke om misbrug af personoplysninger, vil således eventuelt kunne kritiseres for ikke at have levet op til persondatalovens sikkerhedskrav.

Det er i den forbindelse Datatilsynets opfattelse, at nødvendigheden af at undersøge muligt misbrug af adgang til personoplysninger foreligger uafhængigt af, hvilke informationer der i øvrigt måtte være givet hos myndigheden. Efter tilsynets opfattelse kan det derfor ikke nødvendigvis tillægges betydning, om medarbejderne har modtaget forudgående information om en sådan kontrol.

5. Denne udtalelse er alene af vejledende karakter. Datatilsynet må forbeholde sin endelige stillingtagen i tilfælde af en konkret klage- eller tilsynssag.

Med venlig hilsen

Lena Andersen
Kontorchef