Svar (30/5 02)

Videnskabsministeren (Helge Sander):
Datatilsynet har til spørgsmålet udtalt følgende:

Datatilsynet har den 21. maj 2002 præciseret, at offentlige myndigheder – og private virksomheder – har pligt til at træffe særlige foranstaltninger til sikring af personoplysninger, som transmitteres over trådløse netværk, jf. nedenfor under besvarelsen af spørgsmål 2173.

Kontrol af dette forhold vil fremover indgå i Datatilsynets inspektioner hos offentlige myndigheder.

Spm. nr. S 2173

Til videnskabsministeren (21/5 02) af:
Thomas Adelskov (S):
»Findes der i dag et regelsæt eller en vejledning for offentlige myndigheders brug af trådløse datanetværk?«

Begrundelse

I Jyllands-Posten den 19. maj 2002 fremgår det, at kommunernes sikkerhed i forbindelse med brug af trådløse datanetværk er meget ringe. Hvis etableringen af den digitale forvaltning nogensinde skal virkeliggøres, er det vigtigt, at borgerne kan stole på, at sikkerheden er i orden. Derfor vil spørgeren gerne informeres om eventuelle regler eller vejledninger for offentlige myndigheders brug af trådløse datanetværk.

Svar (29/5 02)

Videnskabsministeren (Helge Sander):
Lad mig indledningsvis fastslå, at ansvaret for, at der opretholdes et forsvarligt sikkerhedsniveau hos myndighederne entydigt ligger i den enkelte myndighed. Det er således den enkelte myndigheds ansvar at foretage de fornødne risikoanalyser inden ny teknologi eller nye systemer tages i brug.

Der er ikke fra mit ministerområde udarbejdet regelsæt eller vejledninger for offentlige myndigheders specifikke brug af trådløse datanetværk. Derimod har det tidligere IT-sikkerhedsråd udgivet en generel vejledning i Praktisk brug af kryptering og digital signatur. Denne vejledning fastslår, at der skal anvendes kryptering og digital signatur, hvis kommunikation over *åbne net* skal foregå sikkert med hensyn til autentifikation, integritet og fortrolighed. Vejledningen er bl.a. en hjælp til myndigheder i forbindelse med udarbejdelse af risikoanalyser og afdækning af behov for kryptering af data i kommunikation over åbne net.

Datatilsynet har endvidere til dette spørgsmål udtalt følgende:

Også for offentlige myndigheder gælder bestemmelsen i persondatalovens § 41, stk. 3, om behandlingssikkerhed, jf. herom ovenfor under besvarelsen af spørgsmål 2171.

Endvidere følger det af § 14 i Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelsen), at der kun må etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.

I Datatilsynets vejledning nr. 37 af 2. april 2001 understreges det, at bestemmelsen i sikkerhedsbekendtgørelsens § 14 gælder enhver form for telekommunikation i forbindelse med behandling af personoplysninger. Begrebet »trådløse netværk« er dog ikke nævnt direkte, men dette vil ske i forbindelse med en kommende revision af vejledningen.

Datatilsynet har den 21. maj 2002 præciseret i en vejledende udtalelse, der er offentliggjort på tilsynets hjemmeside (www.datatilsynet.dk), at tilsynet i sikkerhedsmæssig henseende anser et trådløst netværk for en ekstern kommunikationsforbindelse. Datatilsynet har bl.a. anført følgende: »Ved anvendelse af trådløse netværk bør der derfor træffes særlige foranstaltninger med henblik på at sikre data på samme niveau som på et lukket kablet netværk. Eksempelvis vil en sådan beskyttelse kunne bestå i at sikre personoplysninger, som transmitteres over trådløse netværk, efter samme retningslinier, som gælder ved transmission over det åbne internet. Det betyder blandt andet, at der ved transmission af fortrolige oplysninger herunder personnummer skal foretages kryptering, og at følsomme personoplysninger, jf. persondatalovens § 7 og § 8,