Svar (21/12 98)

Kirkeministeren (Marianne Jelved, fg.):
På alle områder skal DNK leve op til de sikkerhedskrav, der i dag stilles til kirkebogsføringen samt de lovgivningsmæssige krav, der i øvrigt måtte være. DNK skal have samme høje sikkerhedsniveau, som er etableret i det nuværende CPR-system og i andre offentlige systemer. Ingen uvedkommende må kunne få adgang til data. DNKs datanet baseres som minimum på lukkede brugergrupper og vil opfylde kravene fra CPR til opkoblede offentlige brugere.

Der skal ikke introduceres en væsentlig større sikkerhed end nu. Det vil i praksis sige, at teknologien ikke skal benyttes som undskyldning for, f.eks. at overvåge kirkebogsførerne nærmere eller fjerne deres generelle adgang til alle informationer i kirkebogen.

Flere kirkekontorer er allerede i dag opkoblet på CPRs forespørgselssystem.

Adgangen til DNK vil mindst have samme høje sikkerhedsniveau, som er etableret i det nuværende CPR-system og i andre offentlige systemer. Ingen uvedkommende vil kunne få adgang til data. Autoriserede brugere vil få adgang til DNK af et personligt password. Der vil ikke ligge data på den lokale pc. Den elektroniske kirkebog vil ikke kunne føres samtidig med at der afvikles andre opgaver, der indebærer en sikkerhedsrisiko.

Endvidere vil brugerne af systemet som hidtil som øvrige offentlige ansatte/tjenestemænd være undergivet tavshedspligt.

Det bemærkes, at der ikke i nyere tid har været tjenstlige sager mod kirkelige medarbejdere i forbindelse med brud på sikkerheden ved kirkebøgernes førelse og ministeriet ser ingen grund til at indførelsen af DNK skulle ændre på dette forhold.

Som nævnt har kun autoriserede brugere adgang til DNK. Der er til i dag ikke konstateret uautoriseret indtrængen i CPR.

Intet bliver slettet i DNK - der er adgang til historik, så hvis nogen fejlagtigt skulle have ændret oplysninger, vil de gamle oplysninger være tilgængelige, og man vil kunne se, hvornår det er blevet ændret og af hvem.

Alle forespørgsler, opdateringer og udskrivninger af attester markeres i den elektroniske kirkebog med tid og bruger. Ingen persondata slettes eller overskrives. Der er kun adgang for autoriserede brugere til gældende registreringer. Ingen data bliver slettet ved opdatering.

For at kunne spore eventuelle forsøg på misbrug af rettighederne til at foretage opslag, vil der i DNK, som det sker i CPR i dag foretages logning af:
- alle forsøg på at komme ind på DNKs fælles database samt
- alle forespørgsler og opdateringer af DNKs fælles database.

Ved logningen registreres tidspunkt, bruger og de aktuelle data.

Den enkelte kirkebogsfører har kun adgang til at tilføre eller rette i den del af kirkebogen, der vedrører hans sogn/sogne.

DNK vil foreligge i flere ens elektroniske versioner ligesom CPR i dag. Endvidere vil der eksternt være sikkerhedskopier. Sandsynligheden for at miste data i DNK er minimal. Originaldata om adresser, CPR-nr, obligationer, aktier m.m. opbevares i dag elektronisk uden at der stilles spørgsmålstegn ved holdbarheden.

Endelig vil DNK-systemet på linie med f.eks. CPR-systemet løbende blive moderniseret og opdateret, således at forældelse ikke bliver en sikkerhedsrisiko.

Ad spm. nr. S 900

Fra miljø- og energiministeren er modtaget supplerende besvarelse af et af Søren Kolstrup stillet spørgsmål. Spørgsmålet er sammen med det foreløbige svar optaget i Folketingstidende 1997-98 (2. samling), forhandlingerne side 2860. Spørgsmålet er desuden supplerende besvaret. Disse svar er optaget i Folketingstidende 1998-99 side 1466 og 2028. Spørgsmålet lød således:

Til miljø- og energiministeren (20/7 98) af:
Søren Kolstrup (EL):
»Vil ministeren oplyse, hvorledes den politiske myndighed er stillet med hensyn til forvaltning af sit politiske mandat, såfremt den private driftsherre af et privatiseret rensningsanlæg går konkurs?«

Supplerende svar (6/1 99)

Miljø- og energiministeren (Svend Auken):
Jeg har forelagt spørgsmålet for Miljøstyrelsen, der har oplyst følgende: