ne af kundgørelse af retsforskrifter omfattet af lovtidendelovens § 2 er knyttet til kundgørelsen i Lovtidende i elektronisk form, jf. herved § 1 a, stk. 2, i udvalgets lovudkast.

Baggrunden herfor er, at Lovtidende efter justitsministerens ikraftsættelse af det vedtagne lovforslag alene vil eksistere i elektronisk form, da der efter det tidspunkt ikke længere vil blive udgivet en Lovtidende i trykt form. Det betyder, at det vil være Lovtidende i elektronisk form, som lovtidendelovens § 3, 1. pkt., henviser til, når det bestemmes, at »offentliggørelse igennem Lovtidende bliver den bindende bekendtgørelsesform«. Heraf følger, at retsvirkningerne af kundgørelse af retsforskrifter omfattet af lovtidendelovens § 2 vil være knyttet til kundgørelsen i Lovtidende i elektronisk form.

3.2. Sikkerhedsforanstaltninger

3.2.1. Tekniske foranstaltninger

3.2.1.1. Udvalgets overvejelser og forslag

Som det fremgår af pkt. 3.1.3.2 ovenfor, har udvalget påpeget, at hensynet til retsanvendelsen kræver, at man med stor sikkerhed kan finde frem til tekster, der entydigt indeholder den autoritative ordlyd af retsforskrifter, som er gældende. Der må derfor tilvejebringes den nødvendige tekniske kapacitet samt tilstrækkelige fysiske og tekniske sikkerhedsforanstaltninger med henblik på at sikre, at et elektronisk kundgørelsessystem har en høj driftssikkerhed og frembyder høj sikkerhed for autenciteten af de kundgjorte retsforskrifter.

Udvalget har nærmere anført, at sikkerhedsniveauet er af afgørende betydning for imødegåelse af risikoen for, at de retsforskrifter, som opbevares og kan søges frem i det elektroniske kundgørelsessystem, er fejlbehæftede f.eks. på grund af fejlindtastninger, systemfejl, strømsvigt eller udefrakommende angreb mod eller manipulation med kundgørelsessystemet. En elektronisk kundgørelsesordning forudsætter derfor en meget høj grad af sikkerhed i de systemer, der anvendes til produktion og formidling af retsforskrifterne.

Udvalget har peget på, at der i forbindelse med elektronisk behandling af oplysninger overordnet kan stilles krav om sikkerhed i tre relationer. For det første skal der være fysisk sikkerhed, således at de lagrede oplysninger befinder sig et aflåst sted, og at der træffes foranstaltninger mod indbrud, brand eller anden fysisk ødelæggelse af dem. For det andet skal der være organisatorisk sikkerhed, hvilket indebærer, at der skal være opbygget rutiner, således at kun autoriserede personer har adgang til oplysningerne, og at disse alene behandles autoriseret. Der skal derfor være fastsat regler og procedurer for, hvilke personer der har adgang til systemet, samt på hvilken måde behandling af oplysninger i systemet må ske. For det tredje skal oplysningerne være sikret systemmæssigt eller teknisk. Denne form for sikkerhed har til formål at hindre at systemet angribes udefra, og at systemet benyttes uautoriseret. Som midler til systemmæssig sikring kan der f.eks. anvendes adgangskoder og registrering af behandlinger, der foretages i systemet (logning).

Om de hensyn, som sikkerhedsforanstaltningerne skal varetage, er nærmere anført følgende:

I forhold til det samlede elektroniske kundgørelsessystem er det anført, at der må stilles krav, som skal skabe sikkerhed for, at det altid er muligt at producere og offentliggøre nye retsforskrifter, således at kundgørelsesproceduren er gennemført og dokumenteret (dvs. registreret) i overensstemmelse med den foreskrevne metode.

Endvidere må der efter udvalgets opfattelse stilles sikkerhedskrav af hensyn til den konkrete tilgængelighed for brugerne af offentliggørelsessystemet. Ved konkret tilgængelighed forstås, at systemerne faktisk er tilgængelige for brugerne. Disse krav skal sikre, at det er muligt at få adgang til de kundgjorte retsforskrifter i det omfang eller tidsrum, som er fastsat. Kravene vedrører systemernes driftssikkerhed i bredeste forstand, og de mest grundlæggende forudsætninger for sikker drift er stabile og robuste edb-programmer, tilstrækkelig teknisk kapacitet i systemet, strenge krav til kvaliteten af driftsmiljøet og opretholdelse af et teknisk beredskab, der gør det muligt hurtigt at konstatere og reagere på systemfejl, driftsforstyrrelser og nedbrud.

Herudover må der stilles krav af hensyn til at sikre retsforskrifternes autenticitet. Disse krav skal skabe sikkerhed for, at retsforskrifterne ikke forvanskes eller tilintetgøres enten på grund af tekniske fejl i processen eller på grund af indgreb fra tredjemand. De ovennævnte forudsætninger for sikker drift medvirker også til at forebygge tekniske fejl, hvorimod der kræves særlige sikkerhedsforanstaltninger for at mindske sandsynligheden for, at angreb udefra kan realiseres. Sådanne sikkerhedsforanstaltninger kan, som det fremgår ovenfor, have karakter af administrative og organisatoriske foranstaltninger, hvilket i denne sammenhæng vil sige etablering af passende regler og forretningsgange, af fysiske sikkerhedsforanstaltninger, f.eks. bygningsmæssige og andre fysiske foranstaltninger til beskyttelse af IT-systemet, og af tekniske sikkerhedsforanstaltninger, dvs. funktionaliteter, som