

eller finder mere begrænset anvendelse. Endelig vil kravene med hensyn til kontrollen i forbindelse med oplysningernes registrering være afhængige af den grad af pålidelighed, der er knyttet til oplysningerne ved indsamlingen.

Efter 2. pkt. skal den myndighed, der er ansvarlig for registeret, endvidere sørge for, at oplysninger, der viser sig at være urigtige eller vildledende, snarest muligt slettes af registeret eller berigtiges. Denne bestemmelse må anses for overholdt, hvis oplysningerne slettes eller berigtiges i forbindelse med den førstkommende normale ajourføring af registeret. For registre, der ikke ajourføres efter en bestemt tidsplan, må rettelsen derimod foretages ved førstgivne lejlighed.

Til § 11.

Efter *stk. 1* skal der træffes de fornødne sikkerhedsforanstaltninger mod, at oplysningerne misbruges eller kommer til uvedkommendes kendskab. Det er ikke anset for muligt i detaljer at beskrive de krav, der i sikkerhedsmæssig henseende må stilles til de enkelte systemer. Den generelle formulering indebærer i øvrigt, at det uden ændring af loven vil være muligt at kræve nye foranstaltninger gennemført i takt med den tekniske udvikling på dette område. Sikkerhedsforanstaltningerne kan bl. a. bestå i *fysisk sikring* (adgangskontrol m. v.) og *systemteknisk sikring* (kendeord, kodning af data m. v.). Forebyggelse mod misbrug kan også ske gennem en *organisatorisk* — *personalemæssig opdeling*, således at de forskellige medarbejdergrupper (systemplanlæggere, programmører, operatører osv.) kun får adgang og kendskab til en del af „registre“.

Forskrifterne for et register skal endvidere indeholde bestemmelser om, hvor registeret må føres, f. eks. i hvilket omfang det må overlades til behandling i et privat edb-servicebureau. Det skal herunder udtrykkeligt være fastsat i forskrifterne, hvis registeret skal overlades til elektronisk databehandling i udlandet, jfr. herved også bestemmelserne i § 19 i forslaget til lov om private registre m. v. om overladelse af særligt følsomme oplysninger om private m. v. til databehandling i udlandet.

Det er en selvfølge, at kravene til sikkerhed mod uretmæssig brug af oplysningerne må variere alt efter oplysningernes karakter. Det er derfor ikke fundet påkrævet at medtage den udtrykkelige bestemmelse i betænkningssudkastets § 13, stk. 2, om særlige sikkerhedsforanstaltninger i forhold til registre, der indeholder sensitive oplysninger som nævnt i forslagets § 9, stk. 2.

Det påhviler den registeransvarlige myndighed og den, der fører registeret, at få gennemført de fornødne sikkerhedsforanstaltninger i overensstemmelse med de fastsatte forskrifter. Registertilsynet kan af egen drift tage spørgsmålet op over for de enkelte registre og med hjemmel i § 26 fremkomme med forslag til regler om yderligere foranstaltninger.

Kravet om gennemførelse af sikkerhedsforanstaltninger refererer sig primært til det sted, hvor registeret teknisk føres, og foranstaltningerne vedrører således navnlig maskiner, programmer og magnetbånd eller -plader m. v. Til en effektiv beskyttelse hører imidlertid også, at der træffes fornødne sikkerhedsforanstaltninger de steder, hvor registermateriale leveres i umiddelbar tilgængelig form (klar tekst), f. eks. som skærmbillede på en dataskærm. I forbindelse med brug af terminaler kan da også indbygges en række systemtekniske sikringer. Bl. a. fordi en modtager af registerudskrifter m. v. som følge af reglerne om videregivelse kan være en anden myndighed end den umiddelbart registeransvarlige myndighed, er der et særligt behov for at kræve sikkerhedsforanstaltninger gennemført hos modtagerne. Hertil kommer, at det i terminalsystemer er almindeligt, at man foruden at fremkalde oplysningerne på en dataskærm samtidig ønsker en papirkopi af skærmbilledet til fortsat brug, f. eks. i forbindelse med patientbehandling på en sygehusafdeling eller i forbindelse med en administrativ sag i kommunalforvaltningen. Det er også nødvendigt, at der fastsættes forskrifter om, at dette materiale efter endt brug destrueres på betryggende måde. Registerudskrifter, der indgår i en administrativ sag, skal dog behandles som sagens øvrige dokumenter.

Derfor fastsættes i *stk. 2*, at sikkerhedsforanstaltningerne også om fornødent skal omfatte kopier og udskrifter af registeret, såvel hos vedkommende myndighed selv som hos andre myndigheder, der modtager kopier af registre eller registerudskrifter. Også her kan der være behov for en forebyggelse gennem en organisatorisk personalemæssig opbygning. Forskrifterne for et register skal således sikre, at kun de sagsbehandlere, der varetager den pågældende opgave inden for myndigheden, får adgang til oplysningerne. Det har navnlig betydning inden for den kommunale administration, hvor hver enkelt kommune varetager en række forskellige forvaltningsopgaver.

I *stk. 3* bestemmes, at der for registre, der indeholder oplysninger af særlig interesse for fremmede magter, skal træffes foranstaltninger, der muliggør registrenes bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.