sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven, jf. lovens § 41, stk. 3. Nærmere regler om sikkerhedskravene i den offentlige forvaltning er fastsat i sikkerhedsbekendtgørelsen, der uddyber kravene til de sikkerhedsforanstaltninger, der kræves efter lovens § 41, stk. 3.

Det følger af sikkerhedsbekendtgørelsens § 11, at kun personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles. Af bestemmelsens stk. 2, fremgår endvidere, at der kun må autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for.

Dette betyder – ifølge Datatilsynets vejledning til sikkerhedsbekendtgørelsen (sikkerhedsvejledningen) – at personer, der ikke er beskæftiget med de formål, hvortil oplysningerne behandles, er uvedkommende i forbindelse med behandlingen, og disse personer må derfor ikke have adgang til oplysningerne. Dette omfatter også øvrige medarbejdere hos den dataansvarlige myndighed.

I forhold til persondatalovens sikkerhedskrav er kriteriet for, om en medarbejder kan få adgang til registrerede personoplysninger således, om medarbejderen har behov herfor i forbindelse med løsningen af de konkrete opgaver, som medarbejderen er beskæftiget med.

Det er den dataansvarlige, der skal meddele autorisationer og i den forbindelse angive, i hvilket omfang medarbejderen må forespørge, inddatere eller slette oplysninger. Den dataansvarlige skal endvidere mindste en gang hvert halve år kontrollere, at de autoriserede personer fortsat opfylder betingelserne for at have adgang til oplysningerne. Den dataansvarlige skal endelig træffe foranstaltninger for at sikre, at kun autoriserede brugere kan få adgang, og at disse kun kan få adgang til de personoplysninger og anvendelser, som de er autoriserede til.

Datatilsynet skal afslutningsvis gøre opmærksom på, at persondatalovens § 10 indeholder en særlig regel, der under visse betingelser gør det muligt at behandle følsomme personoplysninger i videnskabeligt og statistisk øjemed. Behandling efter denne regel kræver anmeldelse til Datatilsynet og udtalelse eller tilladelse fra tilsynet. Datatilsynet stiller endvidere en række vilkår for behandlingen.«

Ad spm. nr. S 4432

Fra justitsministeren er modtaget supplerende besvarelse af et af Anne Baastrup stillet spørgsmål. Spørgsmålet, der sammen med det foreløbige svar er optaget i Folketingstidende 2003-04, forhandlingerne side 12026, lød således:

Til justitsministeren (17/6 04) af:
Anne Baastrup (SF):
»Kan ministeren bekræfte, at flere ansatte ved Biologisk Institut, Aarhus Universitet, har adgang til offentlige registrerede oplysninger om borgerne, og at visse ansatte tillige har adgang til f.eks. politirapporter, straffeattester m.v., og vil ministeren i givet fald begrunde, hvorfor og efter hvilke kriterier adgangen gives?«

Supplerende svar (13/9 04)

Justitsministeren (Lene Espersen):
Justitsministeriet har til brug for besvarelsen indhentet en udtalelse fra Ministeriet for Videnskab, Teknologi og Udvikling, der gennem Aarhus Universitet har indhentet en udtalelse fra Biologisk Institut. Instituttet har i den forbindelse oplyst følgende:

»Biologisk Institut, Aarhus Universitet, skal anføre, at medarbejdere ved instituttet i følge instituttets oplysninger *ikke* har den anførte adgang til de i spørgsmålet anførte registrerede oplysninger om borgerne. For instituttets administrative medarbejdere samt institutledelsen er der i henhold til de generelle retningslinier og procedurer for Aarhus Universitets adgang til privatadresser på medarbejdere og studerende inden for det enkelte institutområde via Aarhus Universitets adgang til CPR-registret, hvilket er den eneste adgang til offentlige registre, der er tale om for institutadministrationen.«
