



IT- og Telestyrelsen
Holsteinsgade 63
2100 København Ø

Sendt til: sagogdokument@itst.dk

19. august 2011

Vedrørende høring over udkast til standarden "Person"

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-post
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2011-122-0673
Sagsbehandler
Kristian Gyde Poulsen
Direkte 3319 3215

1. Ved e-mail af 1. juli 2011 har IT- og Telestyrelsen anmodet Datatilsynet om bemærkninger til udkast til standarden Specifikation for serviceinterface for Person (forkortet "Person").

2. Datatilsynet skal generelt understrege behovet for, at der ved udviklingen af løsninger er opmærksomhed på beskyttelsen af brugernes personlige data og privatliv.

3. Udveksling af personoplysninger mellem offentlige myndigheder skal ske under iagttagelse af persondatalovens¹ regler.

Der må alene ske videregivelse og indsamling af personoplysninger i det omfang, der er hjemmel hertil i behandlingsreglerne i persondatalovens kapitel 4.

Persondatalovens begrænsninger ligger bl.a. i kravet om, at offentlige myndigheder ikke må behandle eller have adgang til oplysninger, som de ikke har behov for i forbindelse med deres konkrete myndighedsudøvelse.

4. Persondatalovens kapitel 11 indeholder regler om behandlingssikkerhed. Det fremgår af persondatalovens § 41, stk. 3, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske 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.

Bestemmelsen i § 41, stk. 3, er nærmere udmøntet i sikkerhedsbekendtgørelsen². Det fremgår af sikkerhedsbekendtgørelsens § 14, 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.

¹ Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer

² Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning

Af Datatilsynets sikkerhedsvejledning³ fremgår, at der ved transmission af fortrolige oplysninger, herunder personnummer, som minimum skal foretages en kryptering.

Datatilsynet skal forslå, at reglerne om behandlingssikkerhed i persondatalovens kapitel 11, herunder kravene til transmission af oplysninger over åbne net, omtales i afsnittet på side 7 om persondatasikkerhed.

5. Af det fremsendte udkast, s. 21, fremgår følgende vedrørende logning:

”Det kræves, at servicen logger alle kald og dataændringer, og gerne at loggen udstilles som en service. Læs mere i ”*Vejledning om ikke funktionelle krav*”.

Datatilsynet forudsætter, at logningskravet i sikkerhedsbekendtgørelsens § 19 ligeledes iagttages i det omfang, de behandlede personoplysninger er omfattet af anmeldelsespligt til Datatilsynet⁴.

Ifølge sikkerhedsbekendtgørelsens § 19 skal der foretages en maskinel registrering (logning) af alle anvendelser af personoplysninger. Registreringen skal mindst indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium.

Med venlig hilsen

Lena Andersen
Kontorchef

³ Vejledning nr. 37 af 2. april 2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning

⁴ Jf. herved persondatalovens kapitel 12