



IT- og Telestyrelsen
Holsteinsgade 63
2100 København Ø

Sendt til: spn@itst.dk

5. november 2007

Vedrørende høring over Dansk SAML 2.0 Profil

Datatilsynet
Borgergade 28, 5.
1300 København K

Ved e-post af 2. oktober 2007 har IT- og Telestyrelsen fremsendt udkast til forslag til Dansk SAML 2.0 Profil (SAML Profile for Deferation in Danish Public Sector V2.0).

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

Det fremgår af beskrivelsen af profilen, at formålet er at definere, hvorledes autentitetssikringsinformation og attributter om brugere kan udveksles mellem IT systemer på en interoperabel og standardiseret måde under hensyntagen til danske forhold som f.eks. OCES digitale signaturer.

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

I høringssvaret tages kun stilling til udkastets afsnit 11.4 med overskriften "Privacy in a Danish Context".

J.nr. 2007-19-0011
Sagsbehandler
Ole Terkelsen
Direkte 3319 3217

Datatilsynet skal bemærke følgende:

Datatilsynet kan konstatere, at omtalen af persondatalovens regler ikke er retvisende, da bl.a. en række af persondatalovens begreber og regler sammenblandes.

Persondatalovens anvendelsesområde

I afsnit 11.4.1 anføres, at offentligt tilgængelige oplysninger ikke er personoplysninger.

Persondataloven¹ gælder ifølge lovens § 1, stk. 1, bl.a. for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling.

Ved "personoplysninger" (eng. "personal data") forstås ifølge lovens § 3, nr. 1, enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede). Offentligt tilgængelige oplysninger kan således også være personoplysninger.

¹ Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger som ændret ved lov nr. 280 af 25. maj 2001.

Generelle behandlingsregler

I afsnit 11.4.1 anføres, at data ikke må registreres, medmindre den dataansvarlige har et ægte behov for at registrere disse. Det er ikke klart, hvad der menes hermed.

Persondatalovens § 5 indeholder en række grundlæggende principper for den dataansvarliges behandling, dvs. indsamling, opbevaring, videregivelse m.v. af personoplysninger.

Af § 5, stk. 2, følger, at indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål, og at senere behandling ikke må være uforenelig med disse formål.

De generelle behandlingsregler i persondatalovens § 5 skal altid være opfyldt.

Opfyldelse af betingelserne i persondatalovens § 5 er dog ikke den eneste forudsætning for behandling af personoplysninger. De nedennævnte behandlingsregler skal tillige være opfyldt.

Følsomme og ikke-følsomme oplysninger

I udkastet synes begreberne ”personoplysninger” og ”følsomme oplysninger” gennemgående at være sidestillet.

Ovenfor er redegjort for begrebet ”personoplysninger”.

Behandlingen af ”følsomme oplysninger” er reguleret i persondatalovens §§ 7-8. I loven benævnes sådanne oplysninger også som oplysninger om rent private forhold (eng. ”purely private data”).

Følsomme er oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold, jf. persondatalovens § 7. Desuden henregnes bl.a. oplysninger om strafbare forhold og væsentligt sociale problemer, jf. lovens § 8, til følsomme oplysninger.

Behandling af ikke-følsomme oplysninger er reguleret i persondatalovens § 6. Dette er oplysninger, som ikke er omfattet af lovens §§ 7-8.

Både følsomme og ikke-følsomme oplysninger kan behandles med et udtrykkeligt samtykke fra den registrerede. Et samtykke skal være frivilligt, specifikt og informeret, jf. persondatalovens § 3, nr. 8. Efter persondatalovens § 38 kan den registrerede tilbagekalde et samtykke.

Som nævnt gælder betingelserne i persondatalovens § 5 ved siden af reglerne i lovens §§ 6-8. Et samtykke er altså ikke i sig selv et tilstrækkeligt grundlag for behandling af personoplysninger.

Datatilsynet skal i øvrigt henlede opmærksomheden på, at det langt fra altid er nødvendigt at indhente et samtykke til behandling af personoplysninger, da der i persondatalovens §§ 6-8 findes en række andre hjemler til behandling.

Behandling af oplysninger om personnummer

I afsnit 11.4. anføres, at personnummer anses for en ”private information”.

Behandling af oplysninger om personnummer er særskilt reguleret i persondatalovens § 11. Der er ikke tale om en følsom oplysning, men derimod om en fortrolig oplysning.

I afsnit 11.4.3 anføres, at et samtykke er nødvendigt for behandling af oplysninger om personnummer.

Offentlige myndigheder kan behandle oplysninger om personnummer med henblik på en entydig identifikation eller som journalnummer, jf. persondatalovens § 11, stk. 1.

Private virksomheder m.v. vil derimod ofte være nødsaget til at indhente samtykke forud for en behandling af oplysninger om personnummer, jf. persondatalovens § 11, stk. 2.

Datatilsynet skal i øvrigt henlede opmærksomheden på, at også med hensyn til behandling af oplysninger om personnummer gælder betingelserne i persondatalovens § 5 ved siden af lovens § 11.

Den registreredes rettigheder – oplysningspligten

Afsnit 11.4.2. synes både at indeholde en omtale af samtykke til behandling af personoplysninger, se herom ovenfor, og reglerne om oplysningspligt. Afsnittet er derfor ikke helt klart. Desuden er det uklart, hvad eksempelvis udtrykket ”general consent-form” indebærer.

Persondatalovens kap. 8-10 omhandler den registreredes rettigheder², herunder oplysningspligten over for den registrerede, jf. lovens kap. 8 (§§ 28-30).

I persondatalovens § 28 reguleres oplysningspligten, hvor oplysningerne indsamles hos den registrerede, mens lovens § 29 omhandler tilfælde, hvor oplysninger ikke indsamles hos den registrerede.

Den registrerede skal efter persondatalovens §§ 28-29 overordnet meddeles de oplysninger, der er nødvendige for, at den registrerede kan varetage sine interesser.

Der findes i persondatalovens kap. 8 en række undtagelser til oplysningspligten.

² Se også Datatilsynets vejledning nr. 126 af 10. juli 2000 om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger.

Behandlingssikkerhed

Behandlingssikkerheden er også omtalt i udkastet. Nedenfor gøres derfor nogle korte bemærkninger herom.

Persondatalovens kapitel 11 indeholder regler om behandlingssikkerhed. I § 41, stk. 1, er det fastsat, at personer, virksomheder m.v., der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, kun må behandle disse efter instruks fra den dataansvarlige, med mindre andet følger af lov eller bestemmelser fastsat i henhold til lov.

Det følger desuden af § 41, stk. 3, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hædeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Der skal således træffes forholdsregler med henblik på at forhindre uvedkommendes adgang til oplysningerne.

For offentlige myndigheder gælder Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.³

Sammenfattende må konstateres, at omtalen af persondatalovens regler ikke er retvisende. Eventuelt kan der i profilen blot henvises til Datatilsynet for nærmere information om persondatalovens regler. Såfremt udkastets afsnit 11.4 med overskriften ”Privacy in a Danish Context” opretholdes, skal Datatilsynet anbefale, at afsnittet omarbejdes, så det bringes i overensstemmelse med persondataloven.

Med venlig hilsen

Ole Terkelsen

³ Bekendtgørelsen og den tilhørende vejledning findes på Datatilsynets hjemmeside, under punktet ”lovgivning”.