DATATILSYNET

IT- og Telestyrelsen
Holsteinsgade 63
2100 København Ø

Sendt til. oiostandarder@itst.dk

28. november 2008

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. 2008-122-0213
Sagsbehandler
Ole Terkelsen
Direkte 3319 3217

Vedrørende høring over FESD GIS-integrationsmodel version 2.0

Ved e-post af 30. oktober 2008 har IT- og Telestyrelsen anmodet om Datatilsynets eventuelle bemærkninger til ovennævnte udkast til standard. Udkastet giver Datatilsynet anledning til følgende bemærkninger:

Af persondatalovens[1] § 41, stk. 3, fremgår, at der skal træffes 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.

I sikkerhedsbekendtgørelsens[2] §§ 11-12 og §§ 16-17 findes nærmere regler om autorisation og adgangskontrol.

Det fremgår af sikkerhedsbekendtgørelsens § 11, stk. 1, at kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles. 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, jf. stk. 2.

Af sikkerhedsbekendtgørelsens § 12, fremgår, at der skal træffes 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.

I udkastet til standard, side 11-12, fremhæves, at der kan være sikkerhedsmæssige problemer ved integrationen mellem ESDH-systemer og GIS:

”2.8 Sikkerhedsforhold
Sikkerhed er et centralt emne ved integration mellem ESDH og GIS, idet ESDH systemer kan indeholde data, som er underkastet forskellige former for fortrolighed, hvorfor adgangsstyring/brugerstyring er meget centralt for ESDH, hvorimod det traditionelt er mindre relevant for GIS-systemer.

[1] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.
[2] Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000, som ændret ved bekendtgørelse nr. 201 af 22. marts 2001, om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

Det er således vigtigt, at ESDH data, der er underkastet restriktioner med hensyn til hvilke brugere, der må få adgang til dem, ikke overføres til GIS-systemer, hvor brugeren typisk kan få adgang til alle data.

Vær opmærksom på, at ESDH systemet, i forbindelse med denne standard, stiller web services til rådighed, der giver mulighed for at hente data ud af systemet, og dermed potentielt også følsomme data. Denne standard indeholder ikke krav til hvordan disse web services sikres mod uautoriseret adgang, men ESDH leverandøren bør overveje at benytte én eller flere af følgende anbefalinger:

- OIO Web SSO Profile 2.0 (også kendt som DK-SAML 2.0).
- Integrated Security (AD)
- IP Adresse beskyttelse (Kun adgang til ESDH web service fra GIS web service)
- OWSA Model T

2.8.1 Samsøgning - sikkerhed
Det primære formål med standarden er at beskrive hvordan ESDH objekter kan stedfæstes geografisk, og således udvide informationerne om sager, dokumenter og parter med denne dimension.

Bindingen mellem et givent ESDH objekt og et geografisk objekt sker gennem anvendelse af en fælles nøgle stedfæstelsesID. GIS systemet og ESDH systemet behøver således ikke have kendskab til hinandens objekter, eller referencer, og i den simpleste form, udgør stedfæstelsen således en mulig udvidelse af informationerne i de to systemer, ved anvendelse af det andet system.

Standarden lægger imidlertid op til at man i GIS systemet gemmer information om et givent objekt. Det vil f.eks. sige at man typebestemmer stedfæstelsen af et ESDH objekt, så man er i stand til at se at der er tale om en sag, uden at skulle hente informationen fra ESDH systemet. Tilsvarende kunne man forestille sig at informationen i GIS systemet omkring en stedfæstet sag, blev udvidet til at indeholde sagstypen. Det ville give mulighed for at foretage søgninger i GIS systemet, f.eks. efter miljøsager i et specifikt geografisk område.

Anvendelsen af denne mulighed introducerer et potentielt problem, i forhold til lovgivning og sikkerhed. GIS systemerne er traditionelt åbne i forhold til de brugere der gives adgang, og har ikke på samme måde en rettighedsmæssig beskyttelse af de enkelte objekter. For en række sagsområder vil det dermed være problematisk at det tillades at foretage søgninger på en sagstype i GIS systemet og få vist eksempelvis hvor der er stedfæstet sager af typen TVANGSFJERNELSE.

Så selvom det åbenlyst vil give en række brugsmæssige fordele, at foretage geografiske søgninger efter ESDH objekter, skal man som myndighed være meget opmærksom på den følsomme information der muligvis vil blive udtrykt åbent i GIS systemet.

Som det fremgår andetsteds i standarden, har der været søgt modeller for at lade standarden beskrive integration mellem GIS og ESDH, på klientniveau, uden held. Tilsvarende er det undersøgt om man på en standardiseret måde kan lade geodata indeholde i FESD Datamodel, med henblik på at lade ESDH systemet tilvejebringe den søgemulighed som er beskrevet ovenfor. Dette har heller ikke vist sig muligt, og det vil således være op til den enkelte myndighed i samarbejde med dennes leverandører af hhv. ESDH og GIS, at løse problemet."

Datatilsynet skal understrege, at persondataloven og sikkerhedsbekendtgørelsen altid skal iagttages, når offentlige myndigheder behandler personoplysninger i it-systemer. Ved en eventuel integration mellem ESDH-systemer og GIS må der ikke skabes mulighed for, at en medarbejder kan tilgå personop-

lysninger, som vedkommende ikke er autoriseret til at have adgang til. Dette gælder både følsomme og ikke-følsomme personoplysninger. Der henvises til sikkerhedsbekendtgørelsens § 12.

Datatilsynet skal desuden særligt henlede opmærksomheden på logningskravet i sikkerhedsbekendtgørelsens § 19, der gælder, når der foretages behandling af personoplysninger omfattet af anmeldelsespligten til Datatilsynet – det vil groft sagt sige, når der er tale om behandling af fortrolige[3] og følsomme personoplysninger.

Det følger af sikkerhedsbekendtgørelsens § 19, stk. 1, at der skal foretages 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. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes. Myndigheder med et særligt behov kan opbevare loggen i op til 5 år.

Datatilsynet skal for en god ordens skyld henlede opmærksomheden på, at enhver behandling – herunder indsamling, samkøring og videregivelse – af personoplysninger skal have hjemmel. En myndighed må f.eks. kun foretage en elektronisk videregivelse af personoplysninger til andre myndigheder eller private, hvis dette er tilladt efter persondataloven eller eventuel særlovgivning på myndighedens område.

Datatilsynet forudsætter, at de enkelte myndigheder *forud* for en eventuel integration mellem deres ESDH-system og GIS drager omsorg for, at integrationen sker under overholdelse af reglerne i persondataloven og sikkerhedsbekendtgørelsen.

Med venlig hilsen

Lena Andersen
Kontorchef

[3] Visse fortrolige personoplysninger kan behandles, uden at det udløser anmeldelsespligt. Se nærmere Justitsministeriets bekendtgørelse nr. 529 af 15. juni 2000 om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for den offentlige forvaltning.