Datatilsynet

Fornyings- og administrasjonsdepartementet
Postboks 8004 Dep
0030 OSLO

Deres referanse	Vår referanse (bes oppgitt ved svar)	Dato
	08/01105-3 /FUE	30. september 2008

Høringsuttalelse - Felles elektronisk tjenesteyting i offentlig sektor

Datatilsynet viser til høringsbrev av 25. juni 2008 vedrørende ovennevnte.

Generelt
Forslaget om en felles IKT-arkitektur omtaler flere elementer innen organisering, beslutninger og koordinering. Datatilsynet har ingen spesifikke merknader til dette.

Forslaget legger opp til en utstrakt sammenstilling av personopplysninger. Det kan innebære uklarhet spesielt med hensyn til ansvar, formål, sikkerhet, datakvalitet og tilgangstyring. Slike sammenstillinger vil uansett måtte innebære kraftige og fungerende tiltak i forhold til nevnte momenter. Datatilsynet har dessverre negative erfaringer i forhold til flere av de tiltak som allerede er initiert, og har dermed økt bekymring i forhold til foreliggende planer. Til sist i brevet nevnes spesifikke kontroller som underbygger tilsynet bekymring.

Datatilsynet ser, i likhet med en rekke andre aktører, en økende trend i forhold til identitetstyveri. Personopplysninger som kommer på avveie, enten som følge av utilsiktet utlevering, uhell eller ved at offentlig sektor tilrettelegger for datainnhøstning, utgjør en viktig parameter i dette trusselbilde. Fellesløsninger for sammenstilling av personopplysninger vil kunne skape ytterlige grobunn for slike hendelser og således skape store utfordringer i forhold til forsvarlig forvaltning av beskyttelsesverdig informasjon i offentlig sektor. Tilsynet synes å se at man i liten grad adresserer slike utfordringer. Rasjonalitet og effektivitet i løsningene kan med en slik mangel gå på forsvarligheten løs. Det innebærer i så fall at den eventuelle gevinsten offentlig sektor oppnår i kort perspektiv, kan få langsiktige skadevirkninger i form av redusert tillit. Det kan blant annet skje dersom man får tilfeller av utilsiktet eller uautorisert utlevering av beskyttelsesverdige opplysninger på grunn av mangelfull forvaltning av personopplysningene.

Fellesløsninger vil også skape store utfordringer i forholdet mellom behandlingsansvarlig, databehandler og eventuelle tredjeparter som er involvert. Det vil også være utfordringer i forhold til skille mellom sensitive og ikke-sensitive personopplysninger. En fellesløsning for offentlig sektor vil generelt si at skille mellom informasjonssikkerhet for sensitive og ikke-sensitive personopplysninger står i fare for å utvannes. Regelverket for det offentlige er også

Postadresse: Postboks 8177 Dep 0034 OSLO | Kontoradresse: Tollbugt 3 | Telefon: 22 39 69 00 | Telefaks: 22 42 23 50 | Org.nr: 974 761 467 | Hjemmeside: www.datatilsynet.no

varierende innenfor de forskjellige sektorer, og dermed kravene til forsvarlig sikring ved behandling av personopplysninger.

Datatilsynet registrerer at informasjonssikkerhet og personvern i hovedsak behandles summarisk og ikke under de respektive punkter hvor dette hadde vært naturlig. De nevnte problemstillinger vil kunne være ulik, avhengig av hvilket trusselbilde som gjør seg gjeldende. Etter tilsynets vurdering må dokumentet styrkes på dette punkt.

Autentisering
Den mest utbredde løsningen for autentisering i offentlig sektor er den som er tilrettelagt fra Skattedirektoratets side. Denne baserer seg på en kombinasjon av PIN-koder og fødselsnummer. Datatilsynet har, som departementet bør være vel kjent med, vært kritisk til denne løsningen i lengre tid. Tilsynets kritiske merknader går spesielt på tre forhold:

- Bruk av en *statsautorisert*, *varig* og *unik* identifikator i påloggingsløsninger er uheldig.
- Distribusjonskanalen for PIN-koder er langt fra tilfredstillende.
- Løsningen er ikke egnet til å beskytte sensitive opplysninger, eller store mengder annen beskyttelsesverdige personopplysninger.

Utover det anfører Datatilsynet også den aggregering av konsekvens en eventuell felles autentisering kan ha, dersom den foreskrevne løsningen blir kompromittert. Slik kompromittering må vurderes både i forhold til løsningen i sin helhet og i forhold til den enkelt bruker. Det er uansett behandlingsansvarliges risikovurdering som må kunne underbygge forsvarligheten i løsningen. Tilsynet ser imidlertid at dette kan være en utfordring, både i forhold til rent tekniske forhold og uklare ansvarsforhold.

Samtrafikknav og meldingsboks
Etableringen av løsning for sentral formidling og lagring av informasjon til den enkelte, skaper en hel del utfordringer. Datatilsynet vil spesielt peke på behandlingsansvar, databehandler og behandlingsgrunnlag. Det sistnevnte vil si at det etter bestemmelsene i personopplysningsloven må etableres et gyldig behandlingsgrunnlag som er tilfredstillende. Dette vil for en fellesløsning av de proporsjoner som skissert her, normalt være i egen lov alternativ et av de andre vilkårene nevnt i lovteksten. Datatilsynet kan imidlertid vanskelig se at personopplysningslovens §§ 8d eller 8f, som ofte anføres i tilsvarende sammenheng, kan legges til grunn.

Datatilsynets kontroller mot Skattedirektoratet og Altinn våren 2008 avdekket en rekke problemstillinger som er relevant i forhold til denne høringen. Likeledes gir kontrollen mot www.norge.no og mot NAV høsten 2007 relevante føringer. Datatilsynet tilråder at disse fire sakene tas med i vurderingen i det videre arbeide. Underlaget kan oversendes på forespørsel.

Med hilsen

for Georg Apenes
direktør

Frank U. Eriksen
Overingeniør