Datatilsynet

Kommunal- og regionaldepartementet
Postboks 8112 Dep

0032 OSLO

Deres referanse	Vår referanse (bes oppgitt ved svar)	Dato
10/2635-2	10/01572-2 /FUE	16. februar 2011

Høringsuttalelse - Forskrift om forsøk med elektronisk stemmegivning under forhåndsstemmegivningen

Det vises til høringsbrev av 16. desember 2010 vedrørende ovennevnte. Datatilsynet har enkelte kommentarer til forslaget, henholdsvis generelle og konkrete.

Generelt
Datatilsynet mener det i utgangspunktet er positivt initiativ å legge til rette for elektronisk stemmegivning. En slik ordning kan inkludere borgere som av ulike årsaker ikke har ønske om eller anledning til å stille i et tradisjonelt valglokale. Videre kan et slikt tiltak ha synergier med hensyn til å fremme bruk av kvalitative e-ID løsninger i samfunnet.

Samtidig er slik ordningen utfordrende i det man introduserer nye problemstillinger. Erfaringer fra andre land vist at det er spesielle utfordringer knyttet til å:

- Autentisere korrekt stemmegiver.
- Verifisere at stemmegiver ikke manipuleres av andre.
- Sikre og forvisse borgeren om at vedkommende deltar i et reelt "hemmelig valg".
- Skape tilstrekkelig tillit til elektroniske systemer. Utfordringen er ikke nødvendigvis å etablere god sikkerhet, men å overbevise borgeren om sådan. Borgeren har verken innsikt i eller forståelse av den tekniske infrastrukturen som benyttes.

Disse utfordringene utelukker imidlertid ikke elektroniske valg som alternativ, men det er viktig at løsningene utvikles i lys av de nevnte erfaringer.

Etter personopplysningslovens definisjon (§ 2), faller politiske oppfatninger inn under kategorien sensitive personopplysninger. Dette får, i den grad personopplysningsloven kommer til anvendelse, konsekvenser for hvilke sikkerhetstiltak som bør iverksettes. Blant

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

annet kan kravene påvirke krav til autentisering, sikring av kommunikasjon og hvordan selve datafangsten sikres.

Datatilsynet vil tilråde at det benyttes instrumenter av høy kvalitet for å sikre at rette vedkommende avgir stemme. Videre at løsningen som "fanger stemmen" reelt sett innfrir forventningen om et "hemmelig valg". Tilsynet ser at det er en rekke praktiske utfordringer i forhold til eventuell ny forhåndstemme, senere oppmøte i valglokale med videre. Det er derfor viktig at departement i den videre prosess søker råd hos fagetatene i forvaltningen.

Utredning av personvernkonsekvensene
Datatilsynet savner at departementet har utredet personvernkonsekvensene av forslaget, jfr. Fornyings- administrasjons og kirkedepartementets veiledning til utredningsinstruksen, "Vurdering av personvernkonsekvenser". Høringsbrevet er forholdsvis knapt og det er vanskelig for tilsynet å vurdere konsekvensene på grunnlag av det utsendte.

Bruk av MinID
Datatilsynet mener at autentisering av stemmegiver bør skje ved bruk av elektronisk signatur, basert på kvalifiserte sertifikater i henhold til lov om digital signatur se også "kravspesifikasjon for PKI i offentlig sektor".

Hva gjelder sikring av selve kommunikasjonen vil ikke tilsynet utelukke at kanalsikring kan være egnet. Dette bør imidlertid utredes nærmere, fortrinnsvis i samråd med relevante fagetater i forvaltningen.

Kobling av personidentitet og avgitt stemme
Slik Datatilsynet forstår løsningen skal en avgitt elektroniske stemme kunne overstyres av en senere avgitt stemme, og i siste instans også overstyres av stemme avgitt i valglokalet. Vi oppfatter det derfor slik at det sentrale systemet har oversikt over hvem som har avgitt hvilken stemme for senere å kunne avlyse/overstyre en tidligere avgitt stemme. Etter tilsynets oppfatning synes det som et usikkerhetsmoment for hemmelig valg, sammenliknet med en papirstemme, at det sentralt i løsningen ligger en koblingen mellom stemmegiver og stemme. Den tradisjonelle papirstemmen og identiteten skilles ad ved stemmegivningen noe vi oppfatter ikke skjer i den elektroniske løsningen.

SMS
Bruk av SMS for å gi tilbakemelding til stemmeangiver vil kreve at mobiltelefonnummer oppgis på forhånd eller inne i selve løsningen for at en SMS løsning skal fungere tilfredstillende. Det å måtte oppgi eget mobilnummer er etter tilsynets oppfatning nok en personopplysing som kan være egnet til å undergrave hensikten med hemmelige valg da dette er en identifikator.

Sikring av brukermiljø
Brukerne av løsningen som benytter den Internett-baserte løsningen for å avgi stemme sitter hjemme på sin egen datamaskin. Det hadde vært ønskelig at løsningen i større grad tok høyde for å sikre brukermiljøet hos hjemmebrukeren, da kompromittering her vil kunne generere falske stemmer, brukerne kan settes under press for å avgi en stemme de ikke ønsker, uvedkommende kan få tilgang til hva som stemmes og løsningen kan bli utsatt for uautoriserte forøk på digitalt innbrudd.

Med hilsen

Bjørn Erik Thon
direktør

Frank U. Eriksen
senioringeniør

Kopi: Fornyings-, administrasjons- og kirkedepartementet,
v/Statsforvaltningsavdelingen,
Pb 8004 Dep, 0030 Oslo