Datatilsynet

Nærings- og fiskeridepartementet
Postboks 8090 Dep
0032 OSLO

Deres referanse	Vår referanse	Dato
15/4361	16/00047-1/EOL	01.03.2016

Datatilsynets høringsuttalelse – Gjennomføring av EUs forordning om eID og elektroniske tillitstjenester

Vi viser til Nærings- og fiskeridepartementets høringsnotat av 30.11.2015 som gjelder gjennomføring av EUs forordning om elektronisk identifisering (eID) og tillitstjenester for elektroniske transaksjoner i det indre marked.

Vi har delt våre merknader inn i tre deler – vår kommentar til om forordningens virkeområde bør avgrenses mot «lukkede systemer», merknader til den delen av høringsnotatet som omhandler eID og merknader til den delen av høringsnotatet som omhandler tillitstjenester.

1. Avgrensning mot «lukkede systemer»

Forordningens virkeområde er i utgangspunktet avgrenset mot det som omtales som «lukkede systemer». Med «lukkede systemer» menes i denne sammenheng frivillige avtaler mellom et begrenset antall deltakere, for eksempel mellom ansatte internt i en virksomhet eller i en medlemsmasse. Det er imidlertid åpning for at nasjonalstatene i gjennomføringen av forordningen kan la den få utvidet virkeområde på dette feltet. Departementet foreslår at «lukkede systemer» ikke skal omfattes av forordningens virkeområde, men heller kan omfattes av en eventuell selvdeklareringsordning.

Da Lov om elektronisk signatur (esignaturloven) skulle vedtas ble det drøftet om såkalt «lukkede systemer» skulle fritas fra kravene til kvalifiserte sertifikater. Den gangen kom man til at alle systemer skulle behandles likt, og at også lukkede systemer måtte oppfylle kravene i esignaturloven. Datatilsynet mener argumentasjonen bak kravet om kvalifiserte sertifikater etter esignaturloven fortsatt er relevant. Grensegangen mellom åpne og lukkede nett er fortsatt uklar. Hvor stor kan f.eks en medlemsmasse være? Kan det være medlemmer av folketrygden?

Datatilsynet mener at i den grad «lukkede systemer» ikke skal omfattes av forordningen må det avklares nærmere hva som kan være et slikt «lukket system». Det bør uansett åpnes for at forordningen også skal gjelde «lukkede systemer» i den grad disse systemene behandler sensitive og beskyttelsesverdige personopplysninger utover i en ren virksomhetsintern kontekst.

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

2. Elektronisk identifisering (eID)

Rene autentiseringsløsninger og krypteringstjenester omfattes ikke av eIDAS-forordningen. Departementet foreslår å opprettholde selvdeklareringsordningen for denne type tjenester. Departementet gir imidlertid ingen nærmere forklaring på hvilke tjenester det her er tale om. Det hadde vært nyttig å få presentert hvilke eksisterende tjenester dette forslaget vil omfatte.

Vi har forståelse for at regelverket skal være teknologinøytralt og løsningsnøytralt, men vi mener samtidig at eksemplifisering er nødvendig for å tydeliggjøre rekkevidden av departementets forslag. Er f.eks ID-porten regnet for å være en ren autentiseringsløsning? I så mener vi det er et betimelig spørsmål om det er tilstrekkelig at ansvarlig myndighet for ID-porten selv skal bestemme sikkerhetsnivå. ID-porten er en nasjonal felleskomponent og en viktig brikke i digitaliseringen av offentlige tjenester. Det er således viktig at det sikres at de totale verdiene denne komponenten har betydning for blir tatt hensyn til.

Digitalt sårbarhetsutvalg har i sin utredning[1] pekt på at dagens IKT-sikkerhetskrav fremstår som fragmenterte og at ulike myndigheter har motstridene prioriteringer med hensyn til sikkerhet. Kjernen i konflikten handler om prinsipielt forskjellig holdning til risikoaksept. I den ene enden finner vi miljøer hvor hovedprioriteten er å hindre uønskede hendelser. I den andre enden finner vi miljøer hvor hovedprioriteten er tilgjengeliggjøring og effektivisering gjennom digitalisering. Difi og NSM er nevnt som eksponenter for hver sin sikkerhetskultur.

Denne konflikten blir særlig problematisk når sikkerhetsnivå i felleskomponenter, som for eksempel ID-porten, skal besluttes. Felleskomponentene er funksjoner som vi har valgt å sentralisere, og som mange virksomheter blir avhengige av. Dersom en felleskomponent som ID-porten har dårlig sikkerhet går sårbarheten i arv til de mange som bruker den, og kan få konsekvenser for mange.

Difi er ansvarlig for drift av ID-porten. Digitalt sårbarhetsutvalg peker på at det er problematisk at offentlige etater alene bestemmer sikkerhetsnivået til felleskomponenter uten at det sikres at de totale verdiene blir tatt hensyn til. Datatilsynet er enig i denne analysen, og mener det er uforsvarlig å ikke regulere krav til sikkerhetsnivå for sentraliserte fellesfunksjoner.

Datatilsynet mener på denne bakgrunn at en selvdeklareringsordning ikke er tilstrekkelig for alle autentiseringsløsninger og krypteringstjenester. De løsninger og tjenester som skal ivareta større verdikjeder må underlegges et regelverk med tydelige krav til sikkerhetsnivå.

NKOM som tilsynsmyndighet
Datatilsynet støtter forslaget om NKOM som tilsynsmyndighet etter eIDAS-forordningen. Departementet bør legge opp til en brukervennlig løsning hva gjelder de meldinger som skal til både NKOM og Datatilsynet.

[1] NOU 2015: 13 Digital sårbarhet – sikkert samfunn – Beskytte enkeltmennesker og samfunn i en digitalisert verden, pkt. 22.6.3

3. Tillitstjenester for elektroniske transaksjoner

En «tillitstjeneste» i eIDAS inkluderer både elektroniske signaturer, elektroniske seil, elektroniske tidsstempler, websideautentisering og elektroniske leveringstjenester. Våre merknader er knyttet til elektroniske leveringstjenester.

Det er et uttalt mål at kommunikasjon primært skal foregå digitalt fremover. Det være seg kommunikasjon mellom offentlige etater, mellom offentlige etater og landets borgere, mellom offentlige etater og aktører i privat næringsliv, mellom aktører i privat næringsliv og landets borgere. Datatilsynet er opptatt av at disse kommunikasjons- og meldingstjenestene skal være underlagt en **forsvarlig regulering med hensyn til ansvar og sikkerhet**. Det vi har sett etter i den nye eID-forordningen og departementets forslag til gjennomføring av forordningen, er hvorvidt dette til sammen utgjør en tilstrekkelig for regulering av alle tjenester for elektronisk kommunikasjon som berører borgerne.

Det er mulig at dette er merknader som går utover det departementet ønsker å få inn i forbindelse med denne høringen som gjelder gjennomføring av eIDAS i norsk rett. Etter vår mening er dette imidlertid kommentarer som er viktig for departementet å ha med seg inn i oppfølgingen av nasjonale tilpasninger som forordningen åpner for.

Etter vår vurdering vil eIDAS kun sørge for forsvarlig regulering av tillitstjenester et stykke på vei. Slik vi forstår eIDAS-forordningens definisjon av «tillitstjeneste» er det kun de kommersielle tilbyderne av elektroniske postkasser som vil være omfattet av regelverket. Det betyr samtidig at den delen av verdikjeden som er statlig, og utenom e-Boks og Digipost, vil falle utenfor. Dette gjelder for eksempel Difis del av Sikker digital post, Altinn og eHelsedirektoratets «Mitt helsearkiv». Dette er tjenester som behandler mye beskyttelsesverdig informasjon om innbyggerne, og vi mener det er en meget utilfredsstillende situasjon at disse gjenstår uten spesifikke krav til ansvar og sikkerhet.

Problembeskrivelse
Digital kommunikasjon er etter 10.02.2014 hovedregelen innenfor forvaltningslovens virkeområde[2]. Digital kommunikasjon er hovedregelen også for kommunikasjon med innbygger.

Digital kommunikasjon skal foregå ved bruk av tjenester som:

- Sikker digital post til innbyggere
- Altinn
- Mitt helsearkiv

Kommersielle tilbydere av elektronisk postkasse til innbyggere er:

- Digipost
- e-Boks

[2] Brev av 10.02.2014 fra statsråd Jan Tore Sanner og KMD.

Slik vi forstår oppbyggingen av de løsninger som er tilgjengelige i dag så er en melding ansett som levert når postkasseleverandør (Digipost/e-Boks) rekrypterer en melding og legger den i mottakers postkasse. På dette tidspunkt er ansvaret regulert i avtalen som er inngått mellom postkasseleverandør og bruker. Ansvarsfordelingen frem til dette skjer fremstår som uklar. Dette er en situasjon vi ikke kan leve med.

Den offentlige felleskomponenten Altinn er primært en plattform for å lage skjema og tjenester. Altinn skal i tillegg brukes for digital post fra forvaltningen til næringsdrivende. Digital post til privatpersoner skal som nevnt gå til Sikker digital post. Likevel er det flere aktører i offentlig sektor som benytter Altinn som digital postkasse for utsendinger til privatpersoner. Dette til tross for at Altinn ikke er bygget med tilstrekkelig sikkerhet for å kunne behandle sensitive og beskyttelsesverdige personopplysninger. Grunnen til dette er at en betydelig del av befolkningen (2, 5 mill) verken har tatt i bruk Sikker digital post eller reservert seg mot denne tjenesten[3].

Løsninger som forvaltningen etablerer for kommunikasjon med privatpersoner vil inneholde sensitive og beskyttelsesverdige personopplysninger (Sikker Digital Post/Mitt helsearkiv). Også kommunikasjon mellom forvalting og næringsliv, samt mellom forvaltningsorganer, vil inneholde sensitive og beskyttelsesverdige personopplysninger (Altinn). Når statlige myndigheter legger opp til at kommunikasjon av denne type opplysninger skal skje digitalt betyr det at de også må sørge for klare ansvarsforhold (hvem har ansvaret når det går galt) og forsvarlig sikkerhet.

Tillitstjeneste uten regulering er ikke tilfredsstillende
eIDAS-forordningen regulerer leveranse av «tillitstjenester» som i definisjonen er beskrevet som en elektronisk tjeneste som normalt utføres mot betaling. Dette indikerer at reglementet er beregnet på tjenester med et kommersielt aspekt. Når det offentlige tilbyr elektroniske tjenester er dette normalt ikke mot betaling. For kommersielle aktører er det imidlertid normalt å ta betalt for slike tjenester – enten uttrykkelig eller innbakt i et kundeforhold ellers. På denne bakgrunn tolker vi det slik at det kun er de kommersielle tilbyderne av elektroniske postkasser som vil være omfattet av regelverket. Dette utgjør i så fall et potensielt lovtomt rom hva gjelder de statlige delene av de elektroniske leveringstjenestene.

Departementet har riktignok uttalt at reglene om sikker meldingsutveksling i eIDAS kan få betydning for den statlige delen av informasjonsformidlingstjensten, nemlig Sikker Digital Post og Altinn[4], men at betydningen vil avhenge av innholdet i Europakommisjonens gjennomføringsrettsakter. Det er 4 gjennomføringsakter knyttet til delen av forordningen som omhandler tillitstjenester (krav til format for eSignatures, krav til format for eSeals, krav til tillitslister, og EU Trustmark), og vi kan ikke se at noen av disse avklarer betydningen av forordningen for Sikker digital post og Altinn. Det er dermed fortsatt uklart hvilken betydning departementet mener forordningen kan få for disse felleskomponentene.

[3] I følge Difi har ca 500 000 personer tatt i bruk Sikker digital post, 90 000 personer har reservert seg og 2.5 mill personer har verken tatt i bruk Sikker digital post eller reservert seg.
[4] EØS-notat av 4. august 2015, www.regjeringen.no/no/sub/eos-notatbasen/sok/id615429/

Denne problemstillingen er for øvrig ikke ny. I 2015 ble det sendt ut på høring en endring av postloven hvor det var foreslått at regulering av digitale posttjenester skulle tas inn, og at NKOM skulle være tilsynsmyndighet. Datatilsynet støttet dette forslaget, men denne delen av lovforslaget ble tatt ut av endelig lovproposisjon. Digital kommunikasjon med innbyggere er i dag ikke regulert i postloven.

Utover de tema som er dekket av gjennomføringsakter fra EU-Kommisjonen er nasjonalstatene gitt et mulighetsrom til å fastsette forskrifter for nasjonal etterfølgelse. Slik vi ser det må Regjeringen sørge for at også den statlige delen av de elektroniske leveringstjenestene har en forsvarlig regulering hva gjelder ansvar og sikkerhet. For å få til dette bør det inntas en hjemmel for forskriftskompetanse for regulering av den statlige delen av Sikker digital post, Altinn, Mitt helsearkiv og evt. andre elektroniske leveringstjenester som måtte komme i fremtiden.

Krav om kvalifiserte tjenestetilbydere
I følge eIDAS forordningen kan Norge selv velge sikkerhetsnivå for tilgang til en tjeneste, samt velge om egne tillitstjenester skal være «kvalifiserte» eller «ikke-kvalifiserte».

Generelt sett er Datatilsynet tilhenger av kvalifiserte tjenester. Dette fordi kvalifisering innebærer en type garanti for sikkerhet som bygger tillit mellom bruker og tilbyder. Det å kreve kvalifisering betyr også at tilbyder har et økonomisk insentiv til regeletterfølgelse fordi manglende regeletterfølgelse kan få erstatningsmessige konsekvenser.

Datatilsynet anmoder Regjeringen om å kreve at alle tilbydere av elektronisk postkasse skal oppfylle kravene til kvalifisert tjenestetilbyder. Dette vil gi bedre forutsigbarhet omkring sikkerhetsnivå og skape den nødvendige tillit til tjenestene. I tillegg vil et krav om å være en kvalifisert tjenestetilbyder gjøre det enklere for den myndighet som skal føre tilsyn etter forordningen, fordi den i større grad kan peke på de spesifikke kravene i forordningen i sin revisjon av tilbyderne.

4. Oppsummering

- Datatilsynet støtter forslaget om NKOM som tilsynsmyndighet etter eIDAS-forordningen.

- Datatilsynet mener det er nødvendig å avklare nærmere hva som ligger i begrepet «lukket system» etter norske forhold dersom slike system ikke skal omfattes av forordningen.

- Datatilsynet mener at en selvdeklareringsordning ikke er tilstrekkelig for alle autentiseringsløsninger og krypteringstjenester. De løsninger og tjenester som skal ivareta større verdikjeder må underlegges et regelverk med tydelige krav til sikkerhetsnivå.

- Departementet må ta med en hjemmel for forskriftskompetanse for regulering av den statlige delen av Sikker digital post, Altinn, Mitt helsearkiv og evt. andre elektroniske leveringstjenester som måtte komme i fremtiden.

- Datatilsynet anmoder Regjeringen om å kreve at alle tilbydere av elektronisk postkasse skal oppfylle kravene til kvalifisert tjenestetilbyder.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Eirin Oda Lauvset
seniorrådgiver

Kopi: Kommunal- og moderniseringsdepartementet
v/Statsforvaltningsavdelingen
Postboks 8112 Dep, 0032 OSLO