DET KONGELIGE
NÆRINGS- OG FISKERIDEPARTEMENT

Prop. 71 LS

(2017–2018)

Proposisjon til Stortinget (forslag til lovvedtak og stortingsvedtak)

Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester), og samtykke til EØS-komiteens beslutning nr. 22/2018 om innlemmelse av forordningen i EØS-avtalen

Innhold

DET KONGELIGE
NÆRINGS- OG FISKERIDEPARTEMENT

Prop. 71 LS

(2017–2018)

Proposisjon til Stortinget (forslag til lovvedtak og stortingsvedtak)

Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester), og samtykke til EØS-komiteens beslutning nr. 22/2018 om innlemmelse av forordningen i EØS-avtalen

Tilråding fra Nærings- og fiskeridepartementet 6. april 2018, godkjent i statsråd samme dag.
(Regjeringen Solberg)

1 Proposisjonens hovedinnhold

EØS-komiteen vedtok ved beslutning nr. 22 av 9. februar 2017 å endre EØS-avtalen vedlegg XI (Elektronisk kommunikasjon, audiovisuelle tjenester og informasjonssamfunnstjenester) ved å innlemme europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner på det indre marked.

Forordningen erstatter europaparlaments- og rådsdirektiv 1999/93/EF (esignaturdirektivet).

Nærings- og fiskeridepartementet foreslår i denne proposisjonen en ny lov for å gjennomføre europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked. Forordningenskal legge til rette for økt elektronisk samhandling mellom næringsdrivende, borgere og offentlige myndigheter på tvers av landegrensene i EU/EØS, og dermed sterkere økonomisk vekst i det indre marked.

Proposisjonen er utarbeidet sammen med Kommunal- og moderniseringsdepartementet (KMD), som er ansvarlig for oppfølgingen av forordningens bestemmelser om gjensidig anerkjennelse av eID, esignatur og elektroniske segl i offentlig sektor.

Forordningen gir Europakommisjonen hjemmel til å gi gjennomføringsrettsakter. Flere slike rettsakter er vedtatt. I denne proposisjonen fore-

slås det at gjennomføringsrettsakter blir norske forskrifter med hjemmel i denne loven.

I kapittel 2 til 3 blir det redegjort for sakens bakgrunn, gjeldende rett og innholdet i forordning (EU) nr. 910/2014. Arbeidet med regelverket i EU og Norge blir omtalt i kapittel 4. I kapittel 6 til 16 følger høringsinstansenes og departementets vurdering av saken, og i kapittel 17 redegjøres det for den lovtekniske gjennomføringen. De økonomiske og administrative konsekvensene forslaget forventes å medføre gjennomgås i kapittel 18. Departementets lovforslag presenteres i kapittel 19.

I EU benyttes ofte forkortelsen «eIDAS-regulation» om forordningen, og kortformen eIDAS brukes enkelte steder i proposisjonen.

Forordning 910/2014 legger til rette for økt elektronisk samhandling mellom næringsdrivende, innbyggere og offentlige myndigheter på tvers av landegrensene i EU/EØS. Forordningen utvider området for reguleringen av elektroniske tillitstjenester sammenliknet med hva esignaturdirektivet omfattet, og styrker dagens regler om elektronisk signatur. Harmonisering av krav til flere typer tillitstjenester kan gjøre det enklere å tilby slike tjenester på tvers av landegrensene. Videre kan strengere krav øke tilliten blant brukerne. Forordningen legger også til rette for at eID-løsninger som oppfyller visse betingelser skal kunne benyttes på tvers av landegrensene. Som det fremgår av forordningens fortale pkt. 12 er målet med dette «[*å*] *sikre at sikker identifikasjon og autentisering er mulig når det gjelder tilgang til nettbaserte tjenester over landegrensene som tilbys av medlemsstatene.*» Reglene i forordningen vil herunder kunne bidra til flere elektroniske transaksjoner på tvers av landegrensene, og i sin tur et mer velfungerende indre marked.

Departementet anser at forordningen er et viktig verktøy i digitaliseringsprosessen, og at den vil bidra til å skape trygghet og tillit på nett. Det nye regelverket skal sikre et felles europeisk rammeverk for regulering av elektronisk signatur og tillitstjenester, og fremme samarbeid på tvers av landegrenser i EU/EØS. Økt bruk av elektronisk kommunikasjon på tvers av landene skal gi mer effektiv samhandling, og på den måten forventes forordningen å bidra til sterkere økonomisk vekst i det indre marked.

1.1 Begreper i proposisjonen

I forordningens artikkel 3 gis det nærmere definisjoner av ord og begreper, og det henvises til denne bestemmelsen for tolkning og nærmere forståelse av forordningens bestemmelser.

I det følgende gis det forklaringer på enkelte begreper som brukes gjennomgående i den videre teksten. Dette er ment som en leseveiledning:

eIDAS er forkortelsen for forordning om «elektronisk identifisering og tillitstjenester for elektroniske transaksjoner i det indre marked».

eID er forkortelsen for elektronisk identifikasjon, som for eksempel BankID og MinID. Begrepet elektroniske identifikasjonsmidler benyttes om dette i forordningen.

PKI (Public Key Infrastructure) – «infrastruktur for offentlig-nøkkel-kryptografi» er en teknologi for å utstede, administrere og bruke eID, esignatur og kryptering basert på en standardisert krypteringsteknologi. I en PKI er den offentlige krypteringsnøkkelen kjent for alle, men kun innehaveren kjenner den private nøkkelen.

Kravspesifikasjon for PKI er en overordnet, funksjonell kravspesifikasjon for selvdeklarering og anskaffelse av PKI-løsninger, herunder PKI-baserte eID-løsninger. Kravspesifikasjonen benyttes i forbindelse med elektronisk kommunikasjon med og i offentlig sektor i Norge.

Standarden brukes i dag for eID på høyeste sikkerhetsnivå i henhold til det norske rammeverket. Offentlig nøkkelteknologi legger til rette for bruk av avanserte elektroniske signaturer og kryptering, ved at brukerne får seg tildelt et elektronisk nøkkelpar som består av en offentlig og en privat nøkkel, og et sertifikat hvor undertegnerens identitet blir knyttet til den offentlige nøkkelen. Den offentlige nøkkelen kan distribueres til mottakerne av de signerte meldingene omtrent som man gjør med telefonnumre. Den private er strengt personlig. Det er altså kun én person som kan signere meldingen ved hjelp av den hemmelige private nøkkelen, mens det er mange som kan bekrefte denne signaturen ved hjelp av den offentlige nøkkelen. Det er også mulig å krypetere ved hjelp av den offentlige nøkkelen; da vil kun innehaveren av den private nøkkelen kunne lese melding. Dette systemet krever en infrastruktur for distribuering av de offentlige nøklene, og denne infrastrukturen omtales gjerne som Public Key Infrastructure (PKI).

Elektronisk signatur er mekanismer som knytter et dokument til en person som signerer dokumentet. Begrepet er teknologinøytralt. For avanserte og kvalifiserte elektroniske signaturer benyttes i praksis PKI-teknologi med sertifikater. En elektronisk signatur kan oppfylle rettslige krav til at et dokument er underskrevet. En elektronisk

signatur bidrar til å sannsynliggjøre opprinnelse og integritet til et dokument.

Elektronisk segl er mekanismer som knytter et dokument til en juridisk person som har forseglet dokumentet. Begrepet er teknologinøytralt. For avanserte og kvalifiserte elektroniske segl benyttes i praksis PKI-teknologi med virksomhetssertifikater. Et elektronisk segl bidrar til å sannsynliggjøre opprinnelse og integritet til et dokument. Begrepet er nytt med eIDAS, og erstatter dagens virksomhetssignaturer.

Et elektronisk sertifikat er en kobling mellom en offentlig nøkkel, identifikasjon (navn) for sertifikatinnehaveren, og eventuelt annen informasjon. Sertifikatet er signert av sertifikatutsteder, som med dette innestår for at sertifikatets innhold er korrekt.

Kvalifiserte sertifikater utstedes av godkjente tilbydere som oppfyller nærmere bestemte krav til rutiner og til virksomheten.

Autentisering brukes primært om å verifisere en påstått identitet. Den som skal autentisere seg, må inneha noe som kan bekrefte identiteten. Dette kalles autentiseringsfaktorer (for eksempel passord, pin-kode-kalkulator eller fingeravtrykk). Ved elektronisk identifikasjon autentiseres en identitetspåstand (for eksempel fødselsnummer) ved bruk av en eID.

Elektroniske tillitstjenester er tjenester som normalt tilbys mot betaling og skal bidra til å styrke tilliten til elektroniske løsninger. eIDAS beskriver tillitstjenestene elektronisk signatur, elektroniske segl, tidsstemplingstjenester, elektronisk tjeneste for registrert sending og sertifikattjenester for nettstedsautentiseringer. Ved å regulere tillitstjenestene vil man oppnå elektronisk samhandling i Europa. Egne tillitstjenester kan også defineres på nasjonalt nivå.

Interoperabilitet er muligheten for et datasystem for å utveksle data og samhandle og fungere med et annet system.

Rammeverk for autentisering og uavviselighet ved elektronisk kommunikasjon i og med offentlig sektor er en retningslinje fastsatt av Fornyings- og administrasjonsdepartementet i 2008. Den definerer fire sikkerhetsnivåer for autentisering med eID, for å gjøre det enklere å gjenbruke autentiseringsløsninger på tvers av offentlige virksomheter og slik gjøre offentlige tjenester enklere å bruke.

Sikkerhetsnivåer: I det norske rammeverket er det i dag definert 4 sikkerhetsnivåer for eID, hvor de to høyeste benyttes i ID-porten. Både nivå 3 og 4 stiller krav om to autentiseringsfaktorer (to-faktor-autentisering). For nivå 4 utleveres eID ved personlig oppmøte og legitimering for å unngå at den havner i feil hender. BankID, Buypass og Commfides leverer eID på dette høyeste nivået. eID på nasjonalt ID-kort vil, når det lanseres, også tilfredsstille det høyeste nivået.

eIDAS-forordningen introduserer tre sikkerhetsnivåer: «lav», «betydelig» og «høy». En gjennomføringsrettsakt til eIDAS inneholder nærmere detaljerte kriterier for disse tre sikkerhetsnivåene. Se nærmere omtale i kapittel 8.

2 Bakgrunnen for lovforslaget

Vi lever i en tid med økende digitalisering, hvor stadig større og viktigere deler av samhandlingen mellom innbyggere, næringsliv og det offentlige finner sted på internett. Som en konsekvens av denne utviklingen melder det seg utfordringer med hensyn til å sikre tillit i digital samhandling. En effektiv og hensiktsmessig digital samhandling forutsetter at alle aktørene har tillit til at elektroniske transaksjoner skjer på en trygg måte. Dersom forbrukeren ikke stoler på den elektroniske betalingsløsningen nettbutikken tilbyr, eller pasienten ikke har tiltro til at medisinen han får utlevert på apoteket, samsvarer med den e-resepten legen sendte, vil det være vanskelig å overbevise partene om å benytte seg av de aktuelle tjenestene.

EU har forsøkt å møte denne utfordringen gjennom forordning 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked. Forordningen ble vedtatt 23. juli 2014, og er basert på et forslag av Europakommisjonen av 4. juni 2012 (COM(2012) 238 final). I fortalen er det uttalt at å sikre tillit på internett er en nøkkel til økonomisk og sosial utvikling. Mangel på tillit gjør at forbrukere, næringslivet og offentlige myndigheter vegrer seg for å gjennomføre elektroniske transaksjoner og å utvikle nye tjenester. I fortalen uttales det også at direktivet om elektronisk signatur ikke har vært et hensiktsmessig verktøy for sikre grensekryssende elektroniske transaksjoner. Forordningen styrker og utvider reglene om elektronisk signatur, regulerer eID og omfatter også andre typer elektroniske tillitstjenester. Begrepet tillitstjenester er nytt og dekker flere tjenester enn de tjenestene som var omfattet av esignaturdirektivet.

I fortalen vises det til «A Digital Agenda for Europe» fra 2010, hvor Europakommisjonen uttaler at mangelen på interoperabilitet og økningen av kriminalitet på internett er to vesentlige hindre mot den «virtuelle syklus» i den digitale økonomien. I rapporten «Dismantling the obstacles to EU citizens' rights» (2010) peker Kommisjonen på behovet for å løse problemene som hindrer EUs borgere i å utnytte fordelene ved et digitalt indre marked og grensekryssende digitale tjenester.

Direktivet om elektronisk signatur oppheves og erstattes av forordningen. I EU gjelder forordningen direkte, og medlemslandene kan ikke gjøre andre nasjonale tilpasninger enn hva som eksplisitt fremgår av forordningen. Ettersom rettsakten er innlemmet i EØS-avtalen har Norge en plikt til å implementere forordningen på tilsvarende måte, men i lovs form.

I høringsnotatet foreslo departementet å gjennomføre forordningen i form av en egen lov om elektroniske tillitstjenester. Det ble også foreslått at gjeldende lov om elektronisk signatur oppheves.

Forordningen er todelt, og inneholder regler som skal legge til rette for:

1. Gjensidig aksept av løsninger for elektronisk identifikasjon (eID) – kapittel II

Gjensidig aksept av løsninger for elektronisk identifikasjon (eID) innebærer at privatpersoner og bedrifter skal kunne bruke sitt elektroniske identitetsbevis (sin eID) for å få tilgang til elektroniske tjenester fra offentlig sektor i andre medlemsland. Dette vil gjøre det enklere å ivareta rettigheter og plikter digitalt på tvers av landegrensene. Kravet om gjensidig aksept gjelder eID-løsninger som har blitt meldt til Europakommisjonen.

Medlemsstaten som har meldt en eID-løsning, må tilby gratis validering av disse eID-ene. Det er frivillig for medlemsstatene å melde eID-løsninger. Plikten til å anerkjenne meldte eID-er gjelder bare tjenester i offentlig sektor. Forordningen gir ikke brukerne rett til nye ytelser, den legger bare til rette for at kommunikasjonen kan skje elektronisk. Forvaltningen kan fortsatt stille vilkår for å få ytelser, og den kan også bestemme hvilket sikkerhetsnivå som anses nødvendig for å få tilgang til en tjeneste. Forordningen innebærer at meldte eID-er på samme nivå skal sidestilles i offentlige tjenester. Det fremgår av fortalen pkt. 17 at medlemsstatene også oppfordres til å muliggjøre bruk av meldte eID-er i privat sektor.

2. Gjensidig aksept av elektronisk signatur og andre tillitstjenester – kapittel III og IV

Forordningen styrker dagens regler om elektronisk signatur (esignatur) og innfører regler om flere typer elektroniske tillitstjenester, deriblant om elektroniske segl, tidsstemplingstjenester, elektronisk tjeneste for registrert sending og sertifikattjenester for nettstedsautentisering. Tilbydere av elektroniske tillitstjenester får flere plikter å forholde seg til, deriblant mer detaljerte krav for identitetskontroll, sikkerhetskrav til virksomheten og opplysningsplikter overfor tilsynsmyndigheten. Det stilles også krav om at utstedere av kvalifiserte tillitstjenester skal revideres av et godkjent revisjonsfirma (samsvarsvurderingsorgan) hvert andre år. Tilbydere av ikke-kvalifiserte tjenester omfattes av deler av regelverket, og tilsynsorganet får nye og mer omfattende håndhevingsoppgaver.

3 Nærmere om forordning (EU) nr. 910/2014

3.1 Formål og virkeområde

Forordningen har til hensikt å sikre et velfungerende indre marked, samtidig som man ivaretar et adekvat sikkerhetsnivå for elektronisk identifikasjon (eID) og tillitstjenester, jf. artikkel 1. Forordningen skal ivareta dette ved å:

- Fastsette på hvilke vilkår medlemsstatene skal anerkjenne elektroniske identifikasjonsmidler for fysiske og juridiske personer som omfattes av en meldt eID-ordning i en annen medlemsstat,
- Fastsette regler for tillitstjenester, spesielt for elektroniske transaksjoner, og
- Etablere et rettslig rammeverk for elektroniske signaturer, elektroniske segl, elektroniske tidsstempler, elektroniske dokumenter, elektronisk tjeneste for registrert sending og sertifikattjenester for nettstedsautentisering.

I art. 2 defineres virkeområdet. Forordningen gjelder for elektroniske identifikasjonsordninger som har blitt meldt inn av en medlemsstat. Videre gjelder den for tilbydere av tillitstjenester som er etablert i unionen. Hva som anses som en tillitstjeneste omtales i punkt 3.3. nedenfor.

Forordningen gjelder ikke for tillitstjenester som utelukkende er brukt innenfor lukkede systemer i henhold til nasjonal lovgivning eller avtale mellom en avgrenset krets av personer. Dette er utdypet i fortalen pkt. 21 på følgende måte:

> «Denne forordning bør særlig ikke omfatte levering av tjenester som utelukkende benyttes i lukkede systemer mellom en definert gruppe av deltakere, og som ikke har noen virkning for tredjemenn. Systemer som er opprettet i foretak eller innen offentlig forvaltning for å håndtere interne prosesser, og der det benyttes tillitstjenester, bør for eksempel ikke omfattes av kravene i denne forordning.»

Forordningen får heller ikke innvirkning på nasjonal rett eller EU-rettslige regler om inngåelse av kontrakter og kontrakters gyldighet, eller andre rettslige og prosessuelle forpliktelser som gjelder formkrav, jf. art. 2 nr. 3.

Indre marked-prinsippet (art. 4)

I artikkel 4 stadfestes «indre marked-prinsippet», som innebærer at tilbydere av tillitstjenester har rett til, uten restriksjoner, å tilby sine tjenester i en annen medlemsstat, når tjenestens formål omfattes av forordningen. Videre skal det være fri bevegelighet for produkter og tjenester som er i samsvar med forordningen i EØS-området.

Personvern (art. 5)

Artikkel 5 nr. 1 fastsetter at behandling av personopplysninger skal skje i samsvar med EUs personverndirektiv (direktiv 95/46/EF)[1]. I fortalen pkt. 11 utdypes dette ved å vise til at autentisering i forbindelse med en online-tjeneste kun skal omfatte behandling av de identifikasjonsdata som er tilstrekkelige, relevante og ikke omfatter mer enn hva som er nødvendig for å gi adgang til den aktuelle tjenesten. Videre er det uttalt at tillitstjenestetilbydere og tilsynsorganer bør oppfylle kravene i direktiv 95/46/EF om konfidensialitet og behandlingssikkerhet. I art. 5 nr. 2 slås det fast at bruken av pseudonym skal være tillatt.

3.2 Elektronisk identifikasjon (kapittel II)

Forordningen innfører en innfører en plikt for offentlige myndigheter til å anerkjenne meldte elektroniske identitetsbevis fra andre medlemsland.

Forordningen definerer tre sikkerhetsnivåer; «lav», «betydelig» og «høy». Anerkjennelsesplikten gjelder for elektroniske tjenester som bruker eID-løsninger på sikkerhetsnivåene betydelig og høy.

---

[1] I 2016 ble direktivet erstattet av EUs personvernforordning (nr. 2016/679) som trer i kraft 25. mai 2018.

Det utenlandske identitetsbeviset må være på et sikkerhetsnivå som er like høyt eller høyere enn det nivået som kreves i den nasjonale tjenesten.

Anerkjennelsesplikten påvirker ikke medlemsstatens rett til å stille krav for å få tilgang til ytelser eller tjenester. Medlemsstaten avgjør også selv hvilket sikkerhetsnivå som skal kreves. Det etableres heller ingen plikt til å melde egne eID-løsninger.

For å sikre tillit til at meldte eID-løsninger har tilfredsstillende sikkerhet er det fastsatt nærmere beskrivelser av sikkerhetsnivåene og prosedyrer for samarbeid mellom medlemslandene både i forbindelse med notifisering og forvaltning av løsningene. Det er også stilt minimumskrav til hvordan personer skal identifiseres.

3.3 Tillitstjenester (kapittel III)

Ved å regulere tillitstjenester legger forordningen til rette for å oppnå elektronisk samhandling mellom innbyggere i Europa. Tillitstjenestene er avgrenset til å omfatte de tjenestene som er tilgjengelige og omsettes på det åpne markedet.

Forordningen styrker eksisterende regler om elektronisk signatur og innfører regler om flere typer elektroniske tillitstjenester. Begrepet «tillitstjenester» er i art. 3 nr. 16 definert som en elektronisk tjeneste som normalt utføres mot betaling, og som består av fremstilling, kontroll og validering av elektroniske signaturer, elektroniske segl eller elektroniske tidsstempler, elektroniske registrerte leveringstjenester og sertifikater knyttet til disse tjenestene, eller fremstilling, kontroll og validering av sertifikater for nettstedsautentisering, eller lagring av elektroniske signaturer, segl eller sertifikater knyttet til disse tjenestene. De fleste kravene i forordningen gjelder for kvalifiserte tillitstjenester, som i art. 3 nr. 17 er definert som tillitstjenester som oppfyller forordningens krav.

3.4 Elektroniske dokumenter (kapittel IV)

Forordningen innfører en regel om at et elektronisk dokument ikke skal nektes rettsvirkning og gyldighet som bevis i forbindelse med rettergang alene av den grunn at det er elektronisk. Dette er allerede etablert praksis i Norge, men ikke i alle EU-land.

4 Arbeidet med regelverket i EU og Norge

Daværende Nærings- og handelsdepartementet (nå Nærings- og fiskeridepartementet) sendte Europakommisjonens forslag til forordning på høring høsten 2012. Hovedinntrykket etter høringen var at høringsinstansene i utgangspunktet var positive til forslaget, samtidig som mange etterlyste viktige avklaringer. Dette gjaldt for eksempel behovet for en nærmere angivelse av sikkerhetsnivå for meldte eID-tjenester og harmoniserte krav til utstedelsesprosedyrer. Videre ble det anført at det å kreve årlig revisjon av sertifikatutstedere var for ofte, og at det ble lagt opp til for mange delegerte rettsakter og gjennomføringsrettsakter, noe som kan svekke forutberegneligheten og klarhet. I høringsrunden kom det også innspill om at forslaget kan få konsekvenser for reglene om ID-kontroll i hvitvaskingsforskriften, forskrift om frivillig selvdeklarasjonsordninger for sertifikatutstedere og Kravspesifikasjon for PKI i offentlig sektor.

I EFTA har forslaget vært fulgt opp av EFTA-arbeidsgruppen for elektronisk kommunikasjon, audiovisuelle tjenester og informasjonssamfunn (WG ECASIS). En felles uttalelse fra EØS/EFTA-landene ble oversendt EU 19. mars 2013, hvor flere av innspillene fra høringsrunden ble tatt med.

En referansegruppe som har bestått av Nærings- og fiskeridepartementet (NFD), Kommunal- og moderniseringsdepartementet (KMD), Justis- og beredskapsdepartementet (JD), Direktoratet for forvaltning og IKT (Difi), Politidirektoratet, Nasjonal kommunikasjonsmyndighet (Nkom) og Brønnøysundregistrene, har fulgt arbeidet med utviklingen av rettsakten. I forbindelse med Kommisjonens arbeid med gjennomføringsrettsakter har også Skattedirektoratet og Nasjonal Sikkerhetsmyndighet deltatt. NFD har løpende orientert bransjen, blant annet på møter i Nkoms «Aktørforum esignatur», og i møter med aktører som BankID, Finans Norge, Commfides og Buypass.

I forbindelse med behandlingen i Rådet og Europaparlamentet, ble Europakommisjonens forslag endret og utdypet på en rekke punkter. Blant annet ble det tatt inn en nærmere angivelse av innholdet i de ulike sikkerhetsnivåene for eID. Forordningen ble publisert i Den europeiske unions tidende 28. august 2014, og trådte i kraft 17. september 2014.

Gjennomføringsrettsakter og delegerte rettsakter

Europakommisjonen startet våren 2014 med å utarbeide gjennomføringsrettsakter som utfyller bestemmelsene i forordningen. Til å bistå, har Kommisjonen etablert «eIDAS Expert Group» der Norge deltar. Norge deltar også som observatør i «eIDAS Committee», som avgir en vurdering av forslaget etter det såkalte komitologisystemet. Frem til dags dato er følgende gjennomføringsrettsakter vedtatt:

- Kommisjonens gjennomføringsbeslutning (EU) 2015/296 av 24. februar 2015 om fastleggelse av prosedyremessige ordninger for samarbeid mellom medlemsstatene om elektronisk identifikasjon etter artikkel 12(7) i europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked.
- Kommisjonens gjennomføringsforordning (EU) 2015/806 av 22. mai 2015 med spesifikasjoner om formatet til EU-tillitsmerke for kvalifiserte tillitstjenester
- Kommisjonens gjennomføringsbeslutning (EU) 2015/1506 av 8. september 2015 om fastsetting av spesifikasjoner vedrørende formater for avanserte elektroniske signaturer og avanserte segl, som skal anerkjennes av offentlige myndigheter i henhold til artiklene 27(5) and 37(5) i europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked.
- Kommisjonens gjennomføringsbeslutning (EU) 2015/1505 av 8. september 2015 om tekniske spesifikasjoner og formater vedrørende tillitslisten i henhold til artikkel 22(5) i europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked.

- Kommisjonens gjennomføringsforordning (EU) 2015/1502 av 8. september 2015 om fastsetting av tekniske minimumsspesifikasjoner og prosedyrer for fastsettelse av sikringsnivåer for elektroniske identifikasjonsløsninger i henhold til artikkel 8(3) i europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked.
- Kommisjonens gjennomføringsforordning (EU) 2015/1501 av 8. september 2015 om interoperabilitetsrammen i artikkel 12(8) i europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked.
- Kommisjonens gjennomføringsbeslutning (EU) 2015/1984 av 3. november 2015 om fastsettelse av vilkår, formater og prosedyrer for notifisering i henhold til artikkel 9(5) i europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked.
- Kommisjonens gjennomføringsbeslutning (EU) 2016/650 av 25. april 2016 om fastsetting av standarder for sikkerhetsvurderinger av kvalifiserte signatur- og seglfremstillingssystemer etter artiklene 30(3) og 39(2) i europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked.

EØS-posisjonsnotater om disse rettsaktene publiseres i EØS-notatbasen fortløpende.

Forordningen inneholder også bestemmelser om gjennomføringsrettsakter og delegerte rettsakter som Kommisjonen «kan» gjennomføre. Dette gjelder blant annet følgende:

- Art. 17 nr. 8 om format og prosedyre for tilsynsorganets rapportering til Kommisjonen
- Art. 19 nr. 4 om sikkerhetstiltak som pålegges virksomhetene
- Art. 20 nr. 4 om akkreditering og regler for revisjon
- Art. 21 nr. 4 prosedyrer ifm. oppstart av en tillitstjeneste
- Art. 24 nr. 5 om etablering av referanser til standarder for sikre («trustworthy») systemer og produkter
- Art. 27 nr. 4 om referanser til standarder for avanserte esignaturer
- Art. 28 nr. 6 om referanser til standarder for kvalifiserte sertifikater.

5 Høringen

Nærings- og fiskeridepartementet sende den vedtatte forordningen på høring 30. november 2015. I høringsnotatet ble det foreslått en ny lov som gjennomfører forordningen, samtidig som lov 15. juni 2001 nr. 81 om elektronisk signatur oppheves. Høringsinstansene ble særlig bedt om å ta stilling til hvorvidt forordningens regler bør få anvendelse på lukkede systemer, om det er behov for å videreføre særhjemmel om esignatur i offentlig sektor, om andre myndigheter enn Nkom bør ha tilsynsoppgavene etter loven, samt hvorvidt selvdeklarasjonsordningen bør beholdes. Fristen for å komme med innspill ble satt til 1. mars 2016. Høringsnotatet ble sendt til følgende instanser:

Departementene
Departementenes sikkerhets- og serviceorganisasjon
Abelia
Accenture
Advokatfirma Ræder DA
Advokatfirmaet Grette DA
Advokatfirmaet Haavind AS
Advokatfirmaet Hjort DA
Advokatfirmaet Thommessen AS
Arbeids- og velferdsdirektoratet
Arntzen De Besche Advokatfirma AS
Atea
Bankenes ID-tjeneste
Bankenes Standardiseringskontor
BankID Norge
Bedriftsforbundet
Bergen kommune
Bing Hodneland Advokatselskap DA
Brønnøysundregistrene
Buypass AS
Cisco Systems Norge
Citrix Systems Norway AS
Commfides Norge
Danske Bank
Datatilsynet
Deltasenteret,
Barne- ungdoms og familiedirektoratet
Den Norske Advokatforening
Den Norske Dataforening
Det Norske Veritas
Direktoratet for forvaltning og IKT (Difi)
Direktoratet for samfunnssikkerhet og beredskap
Direktoratet for økonomistyring
DNB ASA
Domstolene i Norge
Drammen kommune
E-boks
eForum i Standard Norge
Eiendom Norge
Eika Gruppen
Evry
Fagforbundet
Finans Norge
Finanstilsynet
Finn.no AS
Forbrukerombudet
Forbrukerrådet
Funksjonshemmedes Fellesorganisasjon
Fylkesmannen i Sogn og Fjordane
Føyen Advokatfirma DA
Handelshøyskolen BI
Helse Nord RHF
Helse Sør-Øst RHF
Helse Vest RHF
Helsedirektoratet
Helse Midt-Norge RHF
Hovedorganisasjonen Virke
Høgskolen i Gjøvik
IBM Norge
IKT Norge
Innovasjon Norge
Kantega
Kluge Advokatfirma DA
Konkurransetilsynet
Kripos
Kristiansand kommune
KS
Landsorganisasjonen i Norge
Legalteam Advokatfirma DA
Likestillings- og Diskrimineringsombudet
Lotteri- og stiftelsestilsynet
Microsoft Norge
More Software Solutions
Nasjonal kommunikasjonsmyndighet
Nasjonal Sikkerhetsmyndighet
Nasjonalbiblioteket

Nasjonalt ID-senter
Nets Branch Norway
NITO
Nordea Bank Norge ASA
Norges Eiendomsmeglerforbund
Norges Handelshøyskole
Norges teknisk-naturvitenskapelige universitet (NTNU)
Norsk akkreditering
Norsk Regnesentral
Norsk senter for informasjonssikring
Norsk Tipping
NorStella
Norwegian Air Shuttle ASA
NRK
NTT Com Security Norway
Næringslivets hovedorganisasjon
Næringslivets sikkerhetsorganisasjon
Oslo kommune
Politidirektoratet
Posten Norge AS
Programkontoret for nasjonal IKT
Pöyry Management Consulting (Norway) AS
Riksarkivet
Samarbeidsforumet av funksjonshemmedes organisasjoner
Scandinavian Airlines Norge AS
Sem & Stenersen Prokom
Senter for IKT i utdanningen
Sertit
Siemens Norge
Signicat
Simonsen Vogt Wiig
Sintef
Skattedirektoratet
Software Innovation
Sopra Steria
Sparebank 1 Banksamarbeidet DA
Standard Norge
Statens helsetilsyn
Statens Kartverk
Statens Lånekasse for Utdanning
Statoil ASA
Statsbygg
Stavanger kommune
Strålfors
Telenor ASA
TeliaSonera Norge AS
Tenden Advokatfirma ANS
Thales Norway
Trondheim kommune
Uninet Norid AS
Universitetet i Agder
Universitetet i Bergen
Universitetet i Nordland
Universitetet i Oslo – Senter for rettsinformatikk
Universitetet i Stavanger
Universitetet i Tromsø
Utdanningsdirektoratet
Utlendingsdirektoratet
VOX – nasjonalt fagorgan for kompetansepolitikk
Widerøes Flyselskap AS
Wikborg Rein & Co
Økokrim

I alt 41 instanser har uttalt seg. Følgende 26 hadde realitetsmerknader: *Advokatforeningen*, *Brønnøysundregistrene*, *Buypass*, *Commfides*, *Datatilsynet, Direktoratet for e-helse, Direktoratet for forvaltning og IKT, Domstoladministrasjonen, Finans Norge, Finansdepartementet, Forbrukerombudet, Helse Stavanger, Justis- og beredskapsdepartementet, KS, Nasjonal kommunikasjonsmyndighet, Nasjonal sikkerhetsmyndighet, NAV, Norges teknisk-naturvitenskapelige universitet, Politidirektoratet, Posten, Samferdselsdepartementet, Skattedirektoratet, Standard Norge, Statens Kartverk, Trondheim kommune* og *Universitetet i Oslo*

Følgende 15 instanser hadde ikke merknader: *Arbeids- og sosialdepartementet, Departementenes sikkerhets- og serviceorganisasjon, Finanstilsynet, Handelshøyskolen BI, Helse- og omsorgsdepartementet, Helse Vest, Klima- og miljødepartementet, Konkurransetilsynet, Kunnskapsdepartementet, Landbruks- og matdepartementet, Landsorganisasjonen i Norge, Norsk Rikskringkasting AS, Norsk Tipping, Statens pensjonskasse* og *Utenriksdepartementet*.

Inntrykket etter høringen er at høringsinstansene langt på vei stiller seg positive både til innføringen av forordningen med gjennomføringsrettsakter i norsk lov og til samtidig opphevelse av esignaturloven. De fleste instansene som har uttalt seg, gir uttrykk for at de anser forordningen som et viktig verktøy for å understøtte samarbeid og handel mellom aktører i EU/EØS-området, og fremholder at den vil gi norske aktører en mulighet til å nå et større europeisk marked med sine løsninger og tjenester. Flere instanser har imidlertid merknader til forslaget, og det trekkes blant annet frem at de administrative og økonomiske konsekvensene ikke er tilstrekkelig utredet.

Høringsinstansenes innspill og departementets vurdering gjennomgås tematisk i del II nedenfor.

6 Forordningens virkeområde

6.1 Forslaget

I høringsnotatet ble det presisert at det kun er tillitstjenester som tilbys til offentligheten og som har virkning overfor tredjemann, som omfattes av forordningen. Virkeområdet er følgelig avgrenset mot såkalt lukkede systemer. Imidlertid åpnes det for at medlemsstatene i gjennomføringen av forordningen kan la den få utvidet virkeområde også på dette feltet. I høringsnotatet trakk departementet frem forarbeidene til esignaturloven (Ot.prp. nr. 82 (1999–2000) s. 21 flg.) hvor det, under henvisning til forutberegnelighetshensyn og at grensegangen mellom lukkede og åpne nett er uklar, ble konkludert med at også utstedere av kvalifiserte sertifikater innenfor lukkede systemer og som registrerer seg hos tilsynet, skulle omfattes av loven.

Dersom dagens reguleringsmulighet for lukkede systemer mv. ønskes videreført er det et spørsmål om det kan gjøres ved å utvide virkeområdet for kvalifiserte tillitstjenester nasjonalt. Departementet gav i høringsnotatet uttrykk for skepsis med hensyn til en slik utvidelse av virkeområdet, og viste blant annet til at forordningens regulering gir tilbydere av kvalifiserte tillitstjenester vesentlig mer omfattende forpliktelser enn dagens esignaturlov, og omfatter langt flere tjenester. Departementet har derfor foreslått at reglene ikke får anvendelse på lukkede systemer i henhold til nasjonal lovgivning eller avtale mellom en avgrenset krets av personer.

6.2 Høringsinstansenes syn

De fleste instansene som har uttalt seg på dette punkt, deler departementets oppfatning, men flere uttaler at det er behov for en nærmere avklaring av hva begrepet «lukket system» omfatter. *Buypass, Forbrukerombudet, NAV og Politidirektoratet (POD)* er enige med departementet i at forordningens regler ikke bør anvendes på lukkede systemer. Denne oppfatningen støttes også av *Finans Norge* og *BankID*, som påpeker betydningen av en tilstrekkelig klar definisjon. *Datatilsynet* og *Direktoratet for e-helse* presiserer at det foreligger et behov for å avklare grensedragningen mellom lukkede og åpne systemer. Sistnevnte instans fremholder at dersom helsenettet defineres som et lukket system, vil dette kunne gi uheldige konsekvenser i forbindelse med andre regelverk som stiller krav til å bruke kvalifiserte sertifikater eller høyt sikkerhetsnivå, eksempelvis signering av e-resept og autentisering av kjernejournal. *POD* mener at det bør vurderes om ikke bare virksomhetsinterne, men også sektorinterne løsninger kan anses å være lukkede systemer, og viser til løsninger innenfor helse- og omsorgssektoren og internt i offentlig sektor.

Datatilsynet viser til at det i forkant av vedtakelsen av esignaturloven ble drøftet hvorvidt lukkede systemer skulle fritas fra kravene til kvalifiserte sertifikater, og at man den gang besluttet at også lukkede systemer måtte oppfylle lovens krav. *Datatilsynet* mener at argumentasjonen som lå til grunn for dette utgangspunktet, stadig er relevant, og uttaler at det uansett bør åpnes for at forordningen også skal gjelde lukkede systemer, i den grad disse systemene behandler sensitive og beskyttelsesverdige personopplysninger ut over en ren virksomhetsintern kontekst. *NAV* påpeker at det også i lukkede systemer vil være et behov for å ha standarder for tillitstjenester, og anser det som hensiktsmessig om Kravspesifikasjon for PKI i offentlig sektor tilpasses og videreutvikles. *Nasjonal kommunikasjonsmyndighet (Nkom)* kommenterer at dersom forordningens virkeområde ikke utvides, kan dette innebære at enkelte tilbydere som per i dag er registrert som tilbydere av kvalifiserte sertifikater som benyttes internt i virksomheten, i fremtiden ikke vil være å anse som tilbydere av kvalifisert sertifikat, og således heller ikke underlagt tilsyn.

6.3 Departementets vurdering

I forordningens art. 2 nr. 2 fremgår det at den ikke skal få anvendelse på tillitstjenester som utelukkende benyttes i lukkede systemer som følge av nasjonal lovgivning eller avtaler mellom en defi-

nert gruppe av deltakere. Dette er nærmere utdypet i fortalen, hvor det i pkt. 21 presiseres at forordningen særlig ikke bør omfatte «[*l*]*evering av tjenester som utelukkende benyttes i lukkede systemer mellom en definert gruppe av deltakere, og som ikke har noen virkning for tredjemenn. Systemer som er opprettet i foretak eller innen offentlig forvaltning for å håndtere interne prosesser, og der det benyttes tillitstjenester, bør for eksempel ikke omfattes av kravene i denne forordning*.» Departementet forstår det slik at det med dette blant annet tas sikte på å unnta interne systemer som ikke kommuniserer med aktører utenfor den aktuelle virksomheten.

Departementet antar at et system kan regnes for å være lukket også dersom det benyttes av mer enn én virksomhet, og mener at det i vurderingen bør legges vesentlig vekt på om systemet direkte eller indirekte berører tredjepersoner. Det avgjørende er at forordningen ikke kommer til anvendelse når en definert gruppe som kun samhandler seg imellom er enige om hvilken tillitstjeneste de vil anvende internt i gruppen. Et slikt system kan være virksomhetsinternt, uten at dette i seg selv er en forutsetning. For eksempel kan et system for elektronisk meldingsutveksling mellom departementene anses for å være et lukket system, fordi gruppen er forhåndsdefinert og tjenesten ikke benyttes mot tredjeparter.

Departementet er kjent med at den skisserte avgrensningen av forordningens virkeområde vil innebære at en gruppe tilbydere, som i dag er registrert som tilbydere av kvalifiserte sertifikater som benyttes internt i en virksomhet, i fremtiden ikke vil være underlagt tilsyn. Dette dreier seg imidlertid om en liten gruppe tilbydere, og enkelte av disse tilbyderne vil også tilby tjenester som omfattes av forordningens virkeområde, slik at de uansett vil være underlagt tilsyn.

Forordningen regulerer både kvalifiserte og ikke-kvalifiserte tillitstjenester, og dersom lukkede systemer skal omfattes, vil dette innebære en utvidelse av forordningens virkeområde som etter departementets oppfatning ikke korresponderer med regelverkets formål. Departementet anser derfor at det er hensiktsmessig med en avgrensning av lovens virkeområde mot lukkede systemer, og at en slik avgrensning er i tråd med forordningens intensjon og ivaretar hensynet til harmonisering. Departementet mener for øvrig at det ikke nødvendigvis vil være behov for samme grad av tillit og beskyttelse av partene i et internt system, som når en tillitstjeneste skal brukes i det åpne markedet.

7 Selvdeklarasjonsordningen

7.1 Forslaget

Som omtalt i høringsnotatet gir esignaturloven § 16 a hjemmel til å etablere frivillige sertifiserings-, godkjennings- eller selvdeklarasjonsordninger for sertifikatutstedere. Formålet er å høyne sikkerhetsnivået for sertifikattjenester og dermed øke tilliten til og bruken av slike tjenester. Gjennom slike ordninger er det etter dagens regler mulig å stille tilleggskrav ut over de krav som gjelder i esignaturloven for kvalifiserte sertifikater og utstedere av slike. Ordningene vil også kunne stille krav på andre sikkerhetsnivåer.

For eID-løsninger på høyeste sikkerhetsnivå i henhold til Rammeverk for autentisering og uavviselighet[2] er det stilt krav om at løsningen er deklarert i henhold til offentligrettslige krav. En slik selvdeklarasjonsordning er innført for sertifikatutstedere som ønsker å tilby sertifikater i offentlig sektor i henhold til «Kravspesifikasjon for PKI i offentlig sektor». Alle de kommersielle tilbyderne av eID i ID-porten, dvs. BankID, Buypass og Commfides, er selvdeklarert etter denne ordningen. Videre inneholder enkelte forskrifter en henvisning til samme regelsett[3]. I kravspesifikasjonen fremgår det under pkt. 1.3 at selvdeklarerte sertifikatutstedere skal levere basis sertifikattjenester for bruksområdene autentisering og signering med tilhørende statustjenester og oppslagstjenester. Sertifikatutstederne kan velge hvorvidt de vil levere sertifikater for bruksområdet kryptering, og hvilke underliggende tjenester de vil levere.

Når det gjelder kvalifiserte tillitstjenester som er omfattet av forordningen, vil en ordning med selvdeklarasjon ikke oppfylle forordningens krav. Som tidligere nevnt stiller forordningen krav om at det skal foreligge en samsvarsvurdering fra tredjepart, samt en kontroll av denne og registrering hos tilsynsmyndigheten, før tilbyderen kan tilby kvalifiserte tillitstjenester. Dette innebærer med andre ord en *godkjenningsordning*.

Begrepet tillitstjenester er på EU-nivå uttømmende definert i forordningen. Begrepet omfatter blant annet ikke autentiseringstjenester eller krypteringstjenester som sådan, kun de kvalifiserte sertifikater som de eventuelt er basert på. For rene autentiserings- eller krypteringstjenester vil derfor en selvdeklarasjonsordning kunne bidra til å øke tilliten. Videre er ikke forordningens godkjennelsesordning for kvalifiserte tillitstjenester til hinder for at det tilbys frivillige selvdeklarasjonsordninger eller godkjenningsordninger for ikke-kvalifiserte tillitstjenester. Departementet foreslo i høringsnotatet at hjemmelen til å etablere frivillige sertifiserings-, godkjennings- eller selvdeklarasjonsordninger for sertifikatutstedere, beholdes inntil Kommunal- og moderniseringsdepartementets vurdering av Rammeverket og behovet for å beholde Kravspesifikasjon for PKI i offentlig sektor er gjennomført.

7.2 Høringsinstansenes syn

Med hensyn til forslaget om å beholde hjemmelen til å etablere frivillige sertifiserings-, godkjennings- eller selvdeklarasjonsordninger, støttes dette av *Brønnøysundregistrene, Commfides, Direktoratet for e-helse, NAV* og *Nkom*. *Commfides* viser til at det må etableres en god og forutsigbar overgangsordning før dagens selvdeklarasjonsordning eventuelt kan trappes ned. *Direktoratet for e-helse* uttaler at helse- og omsorgssektoren har anskaffet og etablert PKI-løsninger, og at det vil være behov for å vurdere hvilke konsekvenser en avvikling av selvdeklarasjonsordningen vil påføre sektoren før det eventuelt gjøres endringer. *POD* uttaler at hjemmelen for selvdeklarasjonsordningen kan

---

2 Rammeverk for autentisering og uavviselighet ved elektronisk kommunikasjon i og med offentlig sektor. Retningslinjer fastsatt av Fornynings- og administrasjonsdepartementet, april 2008. (Rammeverket er under revisjon.)

3 Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) §36, forskrift om prøveprosjekt for elektronisk kommunikasjon ved tinglysning § 4, forskrift om tiltak mot hvitvasking og terrorfinansiering mv. §5, forskrift om kart, stedfestet informasjon, arealformål og kommunalt planregister (kart- og planforskriften) §10, forskrift om elektronisk kommunikasjon med namsmannen og statens innkrevingssentral i saker etter tvangsfullbyrdelsesloven og i saker for forliksrådet §8, forskrift om forsvars- og sikkerhetsanskaffelser §7-3.

beholdes, da implikasjonene ved å fjerne den ikke er kartlagt. De presiserer imidlertid at en avvikling bør være målet på sikt, blant annet fordi ordningen medfører at utstedere av kvalifiserte sertifikater må registrere seg to ganger hos Nkom, og dermed også betale to gebyrer. *POD* anbefaler videre at kravspesifikasjonen for PKI i offentlig sektor revideres slik at den i størst mulig grad henviser til eIDAS med gjennomføringsrettsakter, og mener det likevel vil være nødvendig med noen få særnorske tilpasninger, for eksempel hvordan en skal kode fødselsnummer i et sertifikat eller avlede fødselsnummeret fra sertifikatet.

BankID, Buypass, Datatilsynet, Finans Norge, Forbrukerombudet og *Nasjonal sikkerhetsmyndighet* mener selvdeklarasjonsordningen bør avvikles. *BankID* og *Finans Norge* påpeker at det ikke er behov for særnorske regler og krav utenfor forordningens reguleringsområde, og foreslår at lovforslagets § 2 strykes. *Buypass* foreslår at eventuelle kompletterende retningslinjer for offentlige tjenesteytere kan fremgå i en ny og oppdatert versjon av «Rammeverk for autentisering og uavviselighet», da med et tydeligere skille mellom bruksområdene autentisering og signering. *Forbrukerombudet* mener at en selvdeklarasjonsordning ved siden av det nye regelverket kan være egnet til å skape uklarhet. *Datatilsynet* og *Nasjonal sikkerhetsmyndighet* finner at selvdeklarasjonsordningen ikke gir tilstrekkelig tillit, og at tjenester som skal ivareta større verdikjeder, må underlegges et regelverk med tydelige krav til sikkerhetsnivå.

7.3 Departementets vurdering

Departementet viser til at en umiddelbar avvikling av selvdeklarasjonsordningen vil kunne få uheldige konsekvenser for de sektorer som benytter etablerte PKI-løsninger. Departementet mener derfor at en eventuell avvikling må foregå gradvis, og først etter at konsekvensene er tilstrekkelig kartlagt.

Departementet mener på den bakgrunn at det er behov for å beholde hjemmelen til å etablere frivillige sertifiserings-, godkjennings- eller selvdeklarasjonsordninger, inntil vurderingen av «Rammeverket for autentisering og uavviselighet» og behovet for å beholde Kravspesifikasjon for PKI i offentlig sektor er gjennomført. Departementet har bedt Nkom om å vurdere PODs merknad vedrørende dobbeltregistrering og betaling for kvalifiserte tilbydere. Nkom opplyser at det ikke må betales to fulle gebyrer, men at gebyret graderes ned for hver registrering fra samme tilbyder.

Selvdeklarasjonsordningen gir i dag et tilsynsregime for kvalifiserte sertifikattjenester som er basert på kravspesifikasjon for PKI. Aktørene erklærer at de etterlever gjeldende kravspesifikasjon for en eller flere sertifikatklasser. Nkom fører tilsyn med etterlevelsen. Forordningens system er at kvalifiserte tillitstjenestetilbydere må ha en tredjepartserklæring (samsvarserklæring) om at tilbyderen oppfyller forordningens krav for tjenesten. Dette er et strengere kontrollregime enn dagens norske krav gir, og dagens selvdeklarasjonsløsning blir da overflødig for de tillitstjenester som forordningen beskriver.

Den norske selvdeklarasjonsordningen brukes i dag blant annet for å etablere eID-løsninger (identifikasjons-/autentiseringstjenester) i Norge. Identifikasjons- og autentiseringstjenester er ikke definert som tillitstjenester i forordningen.

I Norge har vi god erfaring med selvdeklarasjonsordninger. Departementet mener at selvdeklarasjonsordningen fortsatt kan supplere det mer omfattende tilsynsregimet som forordningen legger opp til.

I høringsnotatet ble det foreslått at det kunne etableres ordninger for *tillitstjenester*. Begrepet er definert på EU-nivå i forordningens artikkel 3, og omfatter her et definert antall tjenester. Det er imidlertid forutsatt at medlemsstatene kan definere egne tillitstjenester, jf. gjennomføringsrettsakt 2015/1505 kapittel II. Behovet for selvdeklarasjonsordninger vil primært gjelde for slike tillitstjenester, eksempelvis autentiseringstjenester og krypteringstjenester. For å klargjøre at hjemmelen også dekker nasjonalt definerte tillitstjenester har departementet justert teksten.

Rammeverket er fra 2008 og er under revisjon i lys av eIDAS-forordningen. I den forbindelse vil en også vurdere behovet for kravspesifikasjon PKI for offentlig sektor oghvilke tjenester som i denne omgang bør omfattes av selvdeklarasjonsordningen.

8 Elektronisk identifikasjon

8.1 Gjeldende rett

Elektroniske identitetsbevis (eID) reguleres i dag av Rammeverk for autentisering og uavviselighet ved elektronisk kommunikasjon i og med offentlig sektor, Kravspesifikasjon for PKI[4] i offentlig sektor (v 2.0, juni 2010), selvdeklarasjonsforskriften av 21. november 2005 nr. 1296 og forskrift om utstedere av kvalifiserte sertifikater (begge fastsatt med hjemmel i esignaturloven).

eID brukes for identitetskontroll i elektroniske tjenester. Reguleringen av eID bærer preg av at det er flere aktører som har en rolle i forbindelse med utstedelse og bruk av identitetsbevisene.

Det er den enkelte tjenesteeier som vurderer behovet for sikkerhet og som eventuelt stiller krav om bruk av eID, herunder hvilke eID som kan aksepteres, for tilgang til etatens tjenester, jf. eforvaltningsforskriften § 4. Tjenesteeier «oversetter» sin risikovurdering til et valg mellom de forhåndsdefinerte sikkerhetsnivåene i rammeverket. ID-porten, som muliggjør innlogging til offentlige nett-tjenester, støtter i dag innlogging med eID-er på nivå 3 og 4 etter det norske rammeverket for autentisering og uavviselighet (de to høyeste sikkerhetsnivåene). MinID er på det nest høyeste nivå (nivå 3), mens eID-ene fra BankID, Buypass og Commfides er på det høyeste nivået (nivå 4). Som supplement til markedsaktørene har regjeringen besluttet at politiet skal utstede elektronisk ID (eID) på det høyeste sikkerhetsnivået, når det nasjonale ID-kortet kommer.

8.2 Forslaget

Forordningen etablerer en mulighet for medlemsstatene til å melde sine eID-løsninger til Kommisjonen. Meldte eID-løsninger på sikkerhetsnivåene *betydelig* og *høy* skal gjensidig anerkjennes for tilgang til offentlige nett-tjenester. Anerkjennelsesplikten påvirker ikke medlemsstatens rett til å avgjøre hvilket sikkerhetsnivå som skal kreves for tilgang til tjenestene. Forordningen etablerer heller ingen plikt til å melde egne eID-løsninger.

Forordningen krever ikke i seg selv noen endring i det norske rammeverket, eller i tjenesteeiernes vurdering av hvilket sikkerhetsnivå som skal kreves. Ved eventuell norsk melding av en eID-løsning skal det etableres en knytning mellom sikkerhetsnivået i det norske rammeverket og eIDAS' sikkerhetsnivåer for den meldte eID-løsningen, jf. art. 12 nr. 4 bokstav b. Det bør derfor vurderes nærmere om det er hensiktsmessig med justeringer i rammeverket.

Gjensidig anerkjennelse av eID (artikkel 6)

Plikten til gjensidig anerkjennelse av eID følger av art. 6. Når forvaltningen krever bruk av elektroniske identitetsbevis for å få tilgang til en nett-tjeneste, skal elektroniske identitetsbevis fra medlemslandenes meldte løsninger, gjensidig anerkjennes for grenseoverskridende pålogging til tjenesten. Det utenlandske identitetsbeviset må være på det samme eller ha et høyere sikkerhetsnivå etter forordningen, enn det nivået som brukes i den nasjonale tjenesten. Videre er anerkjennelsesplikten begrenset til offentlige tjenester som bruker elektronisk identitetsbevis på forordningens nivå *betydelig* eller *høy*, jf. forordningens art. 6 nr. 1 bokstav c.

Innholdet i anerkjennelsesplikten er ikke nærmere regulert. I høringsnotatet ga departementet uttrykk for at begrepet «gjensidig anerkjennelse» i utgangspunktet kan oppfattes på to ulike måter: Enten har norske myndigheter bare plikt til å anerkjenne andre EØS-lands notifiserte eID-løsninger etter forordningen dersom også norske løsninger er meldt, eller så har norske myndigheter plikt til å anerkjenne andre EØS-lands meldte eID-løsninger etter forordningen uavhengig av om norske løsninger er meldt.

[4] PKI står for Public Key Infrastructure, offentlig nøkkelinfrastruktur. Den baseres på asymmetrisk kryptering og dekryptering, hvor det er utlevert nøkkelpar bestående av en offentlig og en privat nøkkel; den private nøkkel åpner for dekryptering av innhold som ble kryptert med den offentlige nøkkelen og omvendt.

Notifisering av elektronisk identifiseringsløsning (artikkel 7 og 9)

Artikkel 7 og 9 gir bestemmelser om hvordan elektroniske identifiseringsløsninger skal meldes.

En eID-løsning skal meldes etter en bestemt prosedyre. Kommisjonen offentliggjør og oppdaterer jevnlig en liste over meldte systemer. Medlemsstaten kan også trekke meldinger, slik at de ikke lenger står på listen. Videre vil sikkerhetsbrudd i løsningen kunne føre til at den fjernes fra listen.

Medlemsstaten som melder en eID-løsning, innestår for at personer i løsningen er entydig identifiserte. Videre må medlemsstaten tilby en autentiseringsordning som sørger for at det er mulig for andre medlemsstater gratis å få validert elektroniske identitetsbevis fra løsningen ved bruk mot andre medlemsstaters offentlige tjenester. For eventuell bruk av identitetsbevisene mot privat sektor kan det stilles vilkår og betingelser for tilgang til autentiseringsordningen[5], jf. art. 7 bokstav f, annet ledd og fortalen pkt. 17, tredje punktum. Selve anerkjennelsesplikten gjelder kun for offentlig sektor.

Sikkerhetsnivåer (artikkel 8)

Forordningen definerer i art. 8 tre sikkerhetsnivåer for elektronisk identifisering: *lavt*, *betydelig* og *høyt* sikkerhetsnivå. Kommisjonen har fastsatt nærmere bestemmelser om sikkerhetsnivåene i gjennomføringsrettsakt.[6] Anerkjennelsesplikten gjelder bare for offentlige nett-tjenester som krever innlogging på et av de to høyeste sikkerhetsnivåene. Nivåene er teknologinøytrale, dvs. at de er beskrevet med skjønnspregede begreper, og derfor åpner for at nivåene kan oppnås med ulike teknologier. Både meldingsprosessen og regler om interoperabilitet (art. 12) skal sikre en felleseuropeisk forståelse av nivåene.

Sikkerhetsnivå angis av den medlemsstaten som melder. Ved uenighet, som ikke løses gjennom meldingsprosessen, vil spørsmålet i siste instans måtte avgjøres av EU-domstolen/EFTA-domstolen.

Sikkerhetshendelser (artikkel 10)

Hvis eID-løsningen utsettes for sikkerhetsbrudd, eller på annen måte kompromitteres slik at tilliten til den meldte løsningen svekkes, så har medlemsstaten plikt til å varsle Kommisjonen og medlemsstatene om dette. Løsningen skal også settes ut av drift så langt dette er nødvendig. Hvis manglene ikke utbedres, kan det føre til at den meldte løsningen trekkes fra listen.

Erstatningsansvar (Artikkel 11)

Medlemsstaten, eID-utstederen og autentiseringstjenestetilbyderen vil være erstatningsansvarlig i henhold til nasjonal rett for skader som oppstår på grunn av manglende oppfyllelse av sine plikter etter forordningen. Medlemsstaten har ansvaret for de unike identifiseringsopplysningene som representerer personen og at autentiseringsordningen er tilgjengelig, jf. art. 7 bokstav d og f, mens eID-utstederen er ansvarlig for at det elektroniske identitetsbeviset tildeles den aktuelle personen som opplysningene viser til, jf. art. 7 bokstav e.

Samarbeid og interoperabilitet (artikkel 12)

Forordningen inneholder bestemmelser som skal bidra til teknisk samordning og tillitsbyggende prosesser i forbindelse med gjensidig anerkjennelse av elektroniske identitetsbevis. Det skal etableres et interoperabilitetsrammeverk som skal tilrettelegge for samhandling mellom de ulike meldte eID-løsningene. Rammeverket skal blant annet fastsette tekniske minimumskrav og krav til hvilke identifiserende personopplysninger som minimum skal formidles om personene som identifiseres i meldte eID-løsninger. Videre skal det etableres et samarbeid mellom medlemsstatene om en faglig vurdering («peer review») av eID-løsninger, utveksling av informasjon, erfaringer og god praksis. Gjennomføringsrettsakt 2015/1501 fastsetter nærmere regler for dette. Det fastsettes blant annet et minste datasett som skal overføres for å identifisere innloggede personer. Medlemsstatene må ved melding avgjøre hvordan personen skal identifiseres. Et av spørsmålene vil være om nasjonalt identitetsnummer (for de landene som har det) skal utveksles ved elektronisk autentisering over landegrensene, på samme måte som at numme-

---

5 ID-porten blir den norske autentiseringsordningen. ID-porten benytter i dag eID fra markedet, BankID, Buypass og Commfides, for å gi tilgang på høyeste sikkerhetsnivå.

6 Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

ret i dag fremgår av fysiske identitetsbevis som brukes på tvers av landegrensene. Hvilke identitetsopplysninger som oversendes, vil ha betydning for hvor enkelt personen kan gjenkjennes i den utenlandske tjenesten, og derved også være avgjørende for nytteverdien av den gjensidige anerkjennelsesplikten for eID-er.

For meldte eID-løsninger skal det etableres en knytning mellom sikkerhetsnivåene iht. nasjonalt rammeverk for de meldte eID-løsninger og eIDAS' sikkerhetsnivåer, jf. art. 12 nr. 4 bokstav b.

8.3 Høringsinstansenes syn

Flere høringsinstanser har kommentarer knyttet til anerkjennelsesplikten. *Buypass, POD* og *Justisdepartementet* mener anerkjennelsesplikten bør oppfattes slik at norske myndigheter har anerkjennelsesplikt uavhengig av om norske løsninger er meldte. POD mener at det er mulig å melde en eID-løsning på et lavere nivå enn hva løsningen brukes til nasjonalt.

Advokatforeningen skriver at det er uheldig at det er tolkningstvil om anerkjennelsespliktens utstrekning. *POD* viser i sin høringsuttalelse til at formålet med eIDAS er å tilrettelegge for grenseoverskridende tjenester, og antyder på bakgrunn av dette at det kan finnes nasjonale tjenester som ikke omfattes av anerkjennelsesplikten.

NSM peker på at sikkerhetskravene er beskrevet på overordnet nivå både i EU og i det norske rammeverket, og at det er vanskelig å konkludere med hensyn til om det er sammenfall mellom norsk nivå 4 og eIDAS-nivå *høy*. Et spesifiseringsarbeid er nødvendig før sammenligning kan foretas. *POD* anbefaler at Norge tilpasser kravene til eIDAS-nivåene, slik at vi også nasjonalt benytter eIDAS-sikkerhetsnivåer, i stedet for dagens nivå 3 og 4. Enkelte høringsinstanser mener det kan være behov for et høyere sikkerhetsnivå enn eIDAS høy.

Buypass påpeker at dagens nivå 4 er basert på bruk av kvalifiserte sertifikater for elektronisk signatur, og at en videreføring av en slik knytning til kvalifiserte sertifikater er ønskelig av hensyn til den omfattende sikkerhetsinfrastrukturen i helsesektoren.

POD og *NSM* mener det er nødvendig å etablere en norsk profil som konkretiserer kravene iht. eIDAS sikkerhetsnivåer.

Skatteetaten påpeker at forordningen kun regulerer autentiseringen, når europeiske innbyggere skal anvende offentlige tjenester i andre medlemsstater. Hvordan identifiseringen av personen skal skje, er ikke behandlet i forordningen. De ulike eID-ene autentiserer personen, og bekrefter at oppgitt identifikator er riktig. For de aller fleste offentlige norske tjenester vil det imidlertid også kreves en entydig norsk identifikator.

Flere høringsinstanser har trukket fram utfordringen mht. å knytte eIDAS-innlogginger til identiteter som er registrert i Folkeregisteret. *Brønnøysundregistrene* mener at uten slik knytning vil den gjensidige anerkjennelsen av eID i praksis bli innholdsløs.

POD anbefaler at Norge bør ha som ambisjon å notifisere en e-ID-løsning som gir norske innbyggere mulighet til å gjenbruke sin eID mot europeiske tjenester.

Difi påpeker at det for noen tjenester vil være krav om at den autentiserte kan knyttes til et nasjonalt identitetsnummer. Difi anbefaler også at det må kunne settes minimumskrav til erstatningsansvaret fra eID-utstederen eller medlemsstaten for eventuelt sviktende autentisering. I ID-porten benyttes i dag eID-leverandører som har erstatningsansvar på minst 5 000 kroner eller mer, bl.a. for brudd på pliktene i forbindelse med utstedelse av en eID.

8.4 Departementets vurdering

Forordningen vil kunne gjøre det enklere for innehavere av eID fra andre EØS-land å benytte norske offentlige nett-tjenester som bruker det relevante eIDAS-sikkerhetsnivået. Dette gjelder uavhengig av hvor personen fysisk oppholder seg, med andre ord også personer som fysisk befinner seg i Norge. Ved at de kan gjenbruke sin utenlandske eID, slipper de å skaffe seg et norsk elektronisk identitetsbevis for å benytte tjenestene. Tilsvarende vil norske nettbrukere kunne få mulighet til å gjenbruke sin eID i andre EØS-land. I hvilken grad slike gevinster oppnås, vil bero på hvilke eID-løsninger som meldes, hvilke eIDAS-sikkerhetsnivåer som tas i bruk, og hvordan innloggede brukere vil bli gjenkjent nasjonalt. En god kobling mellom nasjonalt identitetsnummer, som fødselsnummer og d-nummer hos oss, og opplysninger som følger med eID-en som benyttes, vil være en viktig suksessfaktor. For å få nytte av eIDAS må dette arbeidet prioriteres i tiden fremover.

Departementet mener at det bør være en ambisjon for Norge å melde minst én eID-løsning. I forslaget til lov gis Kongen myndighet til å fastsette hvilket organ som skal være meldingsmyndighet overfor Kommisjonen.

Anerkjennelsespliktens omfang

Vilkår for at anerkjennelsesplikten skal inntre er regulert i forordningens art. 6. Bestemmelsen omtaler en gjensidig anerkjennelsesplikt.

Flere høringsinstanser har synspunkter på hvordan den gjensidige anerkjennelsesplikten skal forstås, og at det er uheldig med tolkningstvil. Departementet legger imidlertid til grunn at spørsmålet får liten praktisk betydning, jf. at anerkjennelsesplikten bare gjelder situasjoner hvor virksomheten *bruker* et av de høyeste EU-sikkerhetsnivåene for å gi brukerne tilgang til tjenesten.

Etter departementets syn vil anerkjennelsespliktens nærmere innhold måtte avklares i praksis, og i siste instans av EFTA-/EU-domstolen. Nedenfor redegjøres det for departementets vurdering av innholdet i anerkjennelsesplikten.

Det er på det rene at anerkjennelsesplikten kun gjelder dersom medlemsstaten for den aktuelle tjenesten bruker en eID som er på sikkerhetsnivå *betydelig* eller *høy.* Dette fremgår av forordningen art. 6. Departementet vurderer det slik at det i utgangspunktet er et nasjonalt anliggende å beskrive hvilket nivå en eID-løsning tilfredsstiller, og om det har et tilsvarende eIDAS-nivå. Dersom medlemsstaten mener at det ikke finnes et tilsvarende nivå (eksempelvis at det nasjonale nivået er strengere enn eIDAS høy), vil det etter departementets syn ikke være noen anerkjennelsesplikt for tjenester som krever dette nivået.[7] Ved melding pålegges imidlertid medlemsstaten å etablere en knytning mellom det aktuelle nasjonale sikkerhetsnivået og meldt eIDAS-sikkerhetsnivå. For meldte eID-løsninger foreligger det også et regime for utveksling av informasjon om sikkerhetsnivået blant annet for at det skal kunne foretas en fagfellevurdering fra andre medlemsland, jf. art. 12 nr. 4 bokstav b.

Departementet er enig i at det vil være mulig å melde en eID-løsning på et lavere nivå enn hva den faktisk oppfyller. Ved melding vil imidlertid medlemsstaten være pålagt å knytte sammen nasjonalt sikkerhetsnivå med det meldte nivået, jf. art. 12 nr. 4 bokstav b. Dersom øvrige vilkår i art. 6 er oppfylt, vil det derfor være anerkjennelsesplikt for andre meldte eID-løsninger på samme eller høyere nivå som den meldte.

Forordningen legger opp til at aktørenes erstatningsansvar beror på nasjonal rett. Dagens eID-leverandører i ID-porten har satt ansvarsbegrensninger. Etter gjeldende rett kan forvaltningen stille krav til bruk av sikkerhetstjenester, jf. eforvaltningsforskriften § 4. Departementet ser at det kan være uklarhet med hensyn til om slike krav også kan omfatte minstekrav til eID-leverandørenes erstatningsansvar, og foreslår derfor at spørsmålet kan forskriftsreguleres. Departementet vil presisere at forordningen ikke griper inn i medlemsstatenes rett til å velge sikkerhetsnivå for tjenester.

Virkningen av anerkjennelsesplikten vil i praksis begrenses av at tjenestene som regel har behov for at påloggingen knyttes til en norsk identifikator, og at den innloggede derfor ikke får tilgang før det er etablert en tilfredsstillende knytning til norsk identifikator, jf. venteromsproblematikken omtalt nedenfor.

Eventuell norsk melding

Slik sikkerhetsnivåene er blitt definert, anser departementet det som sannsynlig at Norge vil kunne melde flere eID-løsninger på høyeste eIDAS-sikkerhetsnivå. Det gjelder både eID på nasjonalt ID-kort og markedsløsningene som i dag brukes på sikkerhetsnivå 4 i ID-porten. Før eventuell norsk melding av eID-løsninger må kostnader og nytte ved meldingen vurderes.

I lovforslaget er det foreslått at Kongen fastsetter hvilket organ som skal være meldingsmyndighet overfor Kommisjonen. Det er foreløpig ikke tatt stilling til hvilke eID-løsninger som eventuelt bør meldes, men dette vil skje gjennom meldingsmyndigheten i samarbeid med aktuelle eID-utstedere.

I dag benyttes ID-porten som nav for innlogging til norske offentlige tjenester. Ved en eventuell innlogging med utenlandske meldte eID-er, vil ID-porten validere eID-en mot medlemsstatens gratis autentiseringsordninger. Dersom norske eID-er skal benyttes for innlogging i utenlandske tjenester, vil Norge måtte tilby en tilsvarende gratis autentiseringsordninger i ID-porten.

Sikkerhetsnivåer

I dag benyttes sikkerhetsnivåene fra «Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor». Departementet antar at det vil være relevant å se nærmere på hvorvidt det er behov for å harmonisere rammeverket og de norske sikkerhetsnivåene til eIDAS' sikkerhetsnivåer.

[7] Til støtte for denne tolkningen kan det vises til at eIDAS artikkel 27 nr. 3 uttrykkelig fastsetter at det ikke kan kreves høyere sikkerhetsnivå for signaturer enn kvalifisert signatur, mens det ikke finnes en tilsvarende bestemmelse for eID.

Gjennomføringsrettsakten for sikkerhetsnivåer er vesentlig mer detaljert enn det norske rammeverkets nivåbeskrivelser, men både eIDAS' og norske sikkerhetsnivåer er definert ved hjelp av overordnede og teknologinøytrale krav. Dette er etter departementets syn ønskelig og nødvendig for å tilrettelegge for innovasjon og samspill mellom ulike tekniske løsninger.

Det er per i dag ingen dokumentasjon på at det foreligger et behov for et høyere sikkerhetsnivå enn eIDAS *høyt*. Etter departementets vurdering er det imidlertid ikke noe i veien for at det etableres et høyere nivå nasjonalt, altså at en tjeneste krever eID på et høyere nivå enn hva eIDAS tilbyr.

Identifiseringsutfordringer ved bruk av utenlandske identitetsbevis i Norge (venteromsproblematikken)

Anerkjennelsesplikten innebærer at eID-en skal anerkjennes som et bevis for identiteten til den innloggede, på samme måte som andre identitetsbevis innenfor samme sikkerhetsnivå. Det er imidlertid kun anerkjennelsen av autentiseringen som reguleres direkte av forordningen. Koblingen av identiteten mot nasjonale tjenester er ikke regulert eller løst gjennom forordningen. Dette må det etableres nasjonale løsninger for.

Hvorvidt det er behov for at en innlogget person identifiseres med et nasjonalt identitets-nummer, må tjenesteeierne vurdere. Knytningen til nasjonalt identitetsnummer reguleres ikke av forordningen, og må avklares nasjonalt.

Noen tjenester tilbyr pålogging for personer som ikke er registrert i Folkeregisteret. Slike tjenester vil kunne tilbys for personer som bruker utenlandsk eID selv om vedkommende ikke har en entydig identifikator. De fleste av forvaltningens digitale tjenester baserer seg imidlertid på at personene skal være registrert i Folkeregisteret med fødselsnummer eller d-nummer. Dette er for at man skal kunne gjenkjenne personen fra gang til gang og i ulike sammenhenger.

Forordningens gjennomføringsrettsakt 2015/1501 fastsetter et minste datasett som skal identifisere personen og utleveres ved bruk av eID-en. Fødselsdato, nåværende navn og en unik identifikator er obligatoriske elementer. Det er opp til medlemsstatene å bestemme hvordan den unike identifikatoren skal bygges opp, og om den skal inkludere et identitetsnummer som også brukes i andre sammenhenger, eksempelvis passnummer eller nasjonal identifikator, som svensk personnummer eller samordningsnummer. Valget av identifikator vil ha stor betydning for hvor enkelt det er å gjenkjenne personen for norske tjenester.

Det er en norsk oppgave å finne ut om personen er registrert i Folkeregisteret med fødselsnummer eller d-nummer fra før, og – hvis personen ikke er registrert – om personen skal registreres. Det finnes i dag nasjonale regler om slik registrering i folkeregisterforskriften. Forordningen gir ikke utlendinger flere rettigheter overfor norsk forvaltning enn i dag, og departementet vurderer det slik at forordningen ikke krever endring av dagens regelverk for tildeling av identitetsnumre i Folkeregisteret.

I arbeidet med gjennomføring av forordningen må det ses nærmere på hvordan personer som ikke har et norsk d-nummer eller fødselsnummer, kan gjenkjennes når vedkommende forsøker å identifisere seg med en utenlandsk eID fra en meldt løsning. Hvilke identifiseringsopplysninger som formidles fra autentiseringsordning, vil trolig variere fra medlemsstat til medlemsstat. For autentiseringsordninger som formidler et nasjonalt identitetsnummer for personen, kan det ligge bedre til rette for automatisert gjenkjenning (og knytning til vedkommendes norske identitetsnummer) enn for autentiseringsordninger som kun formidler et løpenummer. Gjenkjenningsutfordringen for identitetsbevis som ikke har norsk identitetsnummer, er i prinsippet den samme for utenlandske eID-er som for fysiske identitetsbevis.

Forordningen regulerer kun plikten til å anerkjenne identitetsbeviset, mens det er opp til Norge å avgjøre hvilke krav som skal stilles for å knytte personen til en identitet i norsk folkeregister. Det fremgår av forordningens fortale avsnitt 14 at anerkjennelsesplikten kun gjelder autentiseringen, mens kravene for tilgang til tjenester beror på nasjonal lovgivning.

I utredningen «Nordic digital identification (eID) – Survey and recommendations for cross border cooperation», som er utarbeidet for Nordisk Ministerråd, omtales dette som «venteromsproblematikken» – brukeren får logget seg på, identitetsbeviset anerkjennes, men brukeren er likevel ikke tilstrekkelig identifisert til å benytte selve tjenesten; personen havner på «venterommet». En av løsningene som vurderes, er at det elektroniske identitetsbeviset inneholder samme identifikatorer som fysiske identitetsbevis og at disse registreres i Folkeregisteret.

Det pågår et samarbeidsprosjekt mellom Difi og Skattedirektoratet for å se på løsninger for dette. I den grad det er behov for endringer i regelverk, vil eventuelle forslag måtte sendes på

høring på vanlig måte. Funn så langt tyder på at noen tjenester vil kunne tilbys innloggede med utenlandske identitetsbevis, selv om personen ikke kan knyttes til en identitet i Folkeregisteret. De fleste tjenester synes imidlertid å forutsette en slik knytning. Det er viktig å finne gode løsninger for dette.

9 Tillitstjenestene

9.1 Gjeldende rett – esignaturloven

Lov 15. juni 2001 nr. 81 om elektronisk signatur (esignaturloven) gir rettslige rammebetingelser for bruk av elektronisk signatur og tilknyttede tjenester. Loven gjennomfører Europaparlaments- og rådsdirektiv 1999/33/EF av 13. desember 1999 om en fellesskapsramme for elektroniske signaturer. Tilsynsmyndighet etter loven er Nasjonal kommunikasjonsmyndighet (Nkom) (som frem til 1. januar 2015 het Post- og teletilsynet).

En elektronisk signatur (esignatur) er i Lov om elektronisk signatur (esignaturloven) § 3 definert som data i elektronisk form som er knyttet til andre elektroniske data, og som brukes som autentiseringsmetode. Esignatur er en generell betegnelse på teknikker for å «signere» digital informasjon på samme måte som en håndskreven signatur benyttes til å undertegne et papirdokument. Disse teknikkene vil eksempelvis kunne være basert på biometriske kjennetegn (fingeravtrykk, avlesing av øye, ansiktsgjenkjenning m.m.), avlesning av en elektronisk penn, eller digitale signaturer basert på elektroniske nøkler og sertifikater. Den tekniske realiseringen av avanserte elektroniske signaturer som kalles digital signatur er for tiden mest utbredt. Ved utforming av digitale signaturer bruker man kryptering som bygger på avanserte matematiske funksjoner.

Bruk av esignatur er egnet til å skape tillit mellom parter som har behov for å vite at den de kommuniserer med, er den som vedkommende gir seg ut for å være. En esignatur kan bidra til å synliggjøre hvem som sendte informasjonen, og at elektronisk overført informasjon ikke har blitt endret underveis. Esignatur kan for eksempel brukes når avtaler inngåsved elektronisk innrapportering, ved elektronisk dokumenthåndtering og ved betaling over internett.

Esignaturloven gjennomfører Europaparlaments- og rådsdirektiv 1999/93/EF av 13. desember 1999 i norsk rett, og gir rettslige rammebetingelser for bruk av elektronisk signatur og tilknyttede tjenester. Loven skiller mellom avanserte og kvalifiserte elektroniske signaturer. En avansert elektronisk signatur er i esignaturloven § 3 nr. 2 definert som en elektronisk signatur som er entydig knyttet til undertegneren, kan identifisere undertegneren, er laget ved hjelp av midler som bare undertegneren har kontroll over, og er knyttet til andre elektroniske data på en slik måte at det kan oppdages om disse har blitt endret etter signering. En kvalifisert elektronisk signatur er i esignaturloven § 3 nr. 3 definert som en avansert elektronisk signatur som er basert på et kvalifisert sertifikat og fremstilt av et godkjent sikkert signaturfremstillingssystem.

I loven § 6 fremkommer det at såfremt lovgivningen åpner for at en disposisjon kan gjennomføres elektronisk, vil et krav om underskrift eller signatur alltid være oppfylt av en kvalifisert elektronisk signatur. Loven presiserer også at andre elektroniske signaturer vil kunne oppfylle et formkrav om håndskreven underskrift.

Det er i dag noe bruk av avansert elektronisk signatur i samfunnet, og da primært basert på kvalifiserte sertifikater. Den største bruken er imidlertid vanlige elektroniske signaturer, altså signaturer som ikke er avanserte. Grunnet prinsippet om formfrihet i norsk avtalerett har det ikke vært behov for en kvalifisert elektronisk signatur, og kostnadene knyttet til et slikt signaturfremstillingssystem er betydelige. Markedet og forvaltningen har følgelig sett seg tjent med å bruke andre elektroniske signaturer.

En elektronisk signatur krever en tilknytning mellom en person og elektroniske data. Elektronisk signatur er i prinsippet et teknologinøytralt begrep. Det er imidlertid allment akseptert at avansert elektronisk signatur i dag kun kan realiseres ved teknologien digital signatur, som innebærer bruk av offentlig nøkkel-kryptografi. En digital signatur krever et elektronisk sertifikat, som i esignaturloven. Esignaturloven § 3 nr. 9 definerer digital signatur som en kobling mellom signaturverifikasjonsdata og undertegner som bekrefter undertegners identitet og er signert av sertifikatutsteder. Sertifikatets viktigste funksjon er herunder å garantere koblingen mellom den private nøkkelen og undertegneren.

I esignaturloven §§ 8 og 9 oppstilles det nærmere krav til sikre signaturfremstillingssystemer.

Per i dag finnes det ikke slike systemer i det norske markedet, og det er ikke innført et system for godkjennelse av slike signaturfremstillingssystemer i Norge. Godkjennelse som er foretatt av et organ i en annen EØS-stat, skal imidlertid likestilles med norsk godkjennelse.

Esignaturloven § 16a gir departementet adgang til å innføre en frivillig sertifiserings-, godkjennings- eller selvdeklarasjonsordning for sertifikatutstedere. Formålet er å øke tilliten til og derved bruken av elektroniske signaturer, jf. Ot.prp. nr. 74 (2004–2005). En selvdeklarasjonsordning er innført for sertifikatutstedere som ønsker å tilby sertifikater i henhold til den til enhver tid gjeldende «Kravspesifikasjon for PKI i offentlig sektor», jf. forskrift 21. november 2005 nr. 1296 om frivillige selvdeklarasjonsordninger for sertifikatutstedere. Gjennom denne ordningen kan en sertifikatutsteder erklære at en sertifikattype som utstederen tilbyr, oppfyller de nærmere angitte kravene.

Lovens § 20 fastsetter at for å sikre at bestemmelser gitt i eller i medhold av loven, kan tilsynet bestemme at sertifikatutsteder skal betale tvangsmulkt. Lovens § 21 pålegger straffeansvar for en kvalifisert sertifikatutsteder som forsettlig eller grovt uaktsomt overtrer plikten til å sende registreringsmelding til tilsynet, unnlater å gi opplysninger eller gir uriktige eller villedende opplysninger til tilsynet, eller behandler personopplysninger i strid med reglene om innsamling, bruk og lagring av opplysninger etter §§ 7 og 14.

Etter esignaturloven § 22 første ledd vil en utsteder av kvalifiserte sertifikater være erstatningsansvarlig for tap hos en fysisk eller juridisk person når denne hadde rimelig grunn til å ha tillit til sertifikatet i henhold til nærmere angitte forhold. Dette gjelder med mindre utstederen godtgjør at han eller hun ikke har handlet uaktsomt (omvendt bevisbyrde).

Esignaturloven § 24 gir hjemmel for å fastsette at registreringspliktige utstedere skal betale gebyr til tilsynet. Gebyrene må ikke overstige kostnadene ved tilsynets virksomhet. Bestemmelser om gebyr er fastsatt i forskrift 21. februar 2005 nr. 168 om gebyr til Post- og teletilsynet § 5. Tilsynet gis adgang til ved enkeltvedtak å «fastsetje årleg gebyr for sertifikatutstedar som er registreringspliktig i samsvar med lov 15. juni 2001 nr. 81 om elektronisk signatur § 18, jf. § 3 og § 24, eller som kjem inn under frivillige sertifiseringsordningar, godkjenningsordningar eller sjølvdeklarasjonsordningar, jf. § 16a og forskrift om frivillige sjølvdeklarasjonsordningar for sertifikatutstedarar § 14.»

9.2 Forslaget

Som nevnt i høringsnotatet legger forordningen til rette for å oppnå elektronisk samhandling mellom innbyggere i Europa ved å regulere tillitstjenester. Tillitstjenestene er avgrenset til å omfatte de tjenestene som er tilgjengelige og omsettes i det åpne markedet.

Forordningen styrker dagens eksisterende regler om elektronisk signatur og innfører regler om flere typer elektroniske tillitstjenester. Begrepet «tillitstjenester» er i art. 3 nr. 16 definert som en elektronisk tjeneste som normalt utføres mot betaling, og som består av fremstilling, kontroll og validering av elektroniske signaturer, elektroniske segl eller elektroniske tidsstempler, elektronisk tjeneste for registrert sending og sertifikater knyttet til disse tjenestene, eller fremstilling, kontroll og validering av sertifikater for nettstedsautentisering, eller lagring av elektroniske signaturer, segl eller sertifikater knyttet til disse tjenestene. Departementet oppfatter listen som uttømmende. Dersom det i fremtiden skulle introduseres nye tillitstjenester som faller under definisjonen i art. 3 nr. 16, anser departementet at disse også vil omfattes av forordningen. Eventuelle fremtidige tjenester som ikke faller under definisjonen, vil kreve egen regulering. De fleste kravene i forordningen gjelder for kvalifiserte tillitstjenester, og disse er i art. 3 nr. 17 definert som tillitstjenester som oppfyller forordningens krav. Det vil i det følgende redegjøres for de ulike tillitstjenestene og hvordan de reguleres i forordningen.

9.2.1 Elektronisk signatur og elektronisk segl

Forordningen etablerer et skille mellom elektronisk signatur (art. 25–34) fra en fysisk person og elektronisk segl (art. 35–40) fra en juridisk person. Forordningen har likelydende bestemmelser for elektronisk signatur og elektronisk segl, men artiklene om rettsvirkninger av de to mekanismene er forskjellige. Alle elektroniske segl skal i utgangspunktet kunne føres som bevis, og for kvalifiserte elektroniske segl skal det antas at integriteten til dataene som det kvalifiserte elektroniske seglet er knyttet til, er intakt og at dataenes opprinnelse er riktige.

Forordningen stiller de samme vilkårene som direktiv 1999/93/EF for hva som skal anses som en avansert elektronisk signatur, og stiller tilsvarende krav for hva som skal anses som et avansert elektronisk segl. Vilkårene sikrer at signaturen/seglet entydig kan knyttes til og identifisere

undertegneren eller skaperen av seglet, at signaturen/seglet er laget kun ved hjelp av midler som vedkommende har kontroll over og er knyttet til andre elektroniske data slik at det oppdages om disse er endret etter signering. Det fremgår av fortalen avsnitt 58–59 at segl vil dannes av juridiske personer, mens fysiske personer signerer.

Et kvalifisert elektronisk sertifikat kan være en bestanddel for å lage en avansert elektronisk signatur eller et avansert elektronisk segl. Forordningen stiller krav gjennom art. 28 og 38 til kvalifiserte sertifikater som sikrer identifisering av innehaveren av sertifikatet, og på den måten gir sikkerhet for at signaturen eller seglet virkelig tilhører vedkommende. En avansert elektronisk signatur basert på et kvalifisert sertifikat og som er fremstilt av et kvalifisert elektronisk signaturfremstillingssystem gir en kvalifisert elektronisk signatur. Tilsvarende vil et avansert elektronisk segl basert på et kvalifisert sertifikat og som er fremstilt av et kvalifisert elektronisk seglfremstillingssystem, gi et kvalifisert elektroniske segl.

Gjennom forordningens art. 29 og vedlegg II til forordningen stilles det krav til det kvalifiserte elektroniske signaturfremstillingssystemet. Dette systemet skal blant annet sikre at de elektroniske signaturfremstillingsdataene med rimelig sikkerhet er konfidensielle og kun kan forekomme én gang. Systemet skal også sikre at de elektroniske signaturfremstillingsdataene som anvendes, ikke kan utledes, og at den elektroniske signaturen er beskyttet mot forfalskning og andres bruk. Kommisjonen kan fastsette gjennomføringsrettsakter hvor det oppstilles referansenummer til standarder for kvalifiserte elektroniske signaturfremstillingssystemer.

Videre skal et kvalifisert elektronisk signaturfremstillingssystem sertifiseres i henhold til art. 30 i forordningen. Medlemslandene skal melde fra til Kommisjonen om hvilket organ som skal foreta en slik sertifisering og hvilke systemer som har blitt sertifisert. Kommisjonen skal lage en offentlig tilgjengelig oversikt over sertifiserte signaturfremstillingssystemer, jf. art. 31. Etter art. 39 gjelder art. 29–31 tilsvarende for kvalifiserte systemer for fremstilling av elektroniske segl.

Sertifiseringen av kvalifiserte elektroniske signaturfremstillingssystemer skal etter art. 30 pkt. 3 basere seg på refererte standarder fastsatt ved gjennomføringsrettsakt fra Kommisjonen. Fortalens pkt. 55 uttaler at IT-sikkerhetssertifiseringen bør baseres på internasjonale standarder, som for eksempel ISO/IEC 15408, og dertil tilknyttede evalueringsmetoder og gjensidige anerkjennelsesordninger. Alternative evalueringsprosesser skal kun benyttes for evaluering av teknologiske løsninger hvor det ennå ikke er utarbeidet eller fastsatt en standard som disse systemene kan evalueres etter. Alternative evalueringsprosesser skal så langt som mulig være sammenlignbare med allerede fastsatte standarder for IT-sikkerhetssertifisering.

Forordningen stiller i art. 32 krav til valideringen av en kvalifisert elektronisk signatur for å kunne fastslå gyldigheten av signaturen på signeringstidspunktet. Blant annet skal valideringen bekrefte at det kvalifiserte sertifikatet var gyldig og utstedt av en kvalifisert tillitstjenestetilbyder på signeringstidspunktet. I art. 33 stilles det også krav til den som tilbyr en kvalifisert valideringstjeneste for kvalifiserte elektroniske signaturer, som for eksempel at valideringen skal utføres i henhold til art. 32 pkt. 1. Artikkel 32 og 33 gjelder også for validering av kvalifiserte elektroniske segl, jf. art. 40.

En kvalifisert tillitstjenestetilbyder som tilbyr lagringstjeneste for kvalifiserte elektroniske signaturer og segl, må kunne sikre rettsvirkningene av den elektroniske signaturen eller seglet over et lengre tidsrom og garantere at de kan valideres uavhengig av teknologisk utvikling, jf. art. 34 og 39.

For art. 28–34 og 37–38 kan Europakommisjonen blant annet fastsette gjennomføringsrettsakter som definerer referansestandarder for de ulike kravene til elektroniske signaturer og elektroniske segl. Etter art. 30 kan Europakommisjonen fastsette en delegert gjennomføringsrettsakt med kriterier til det organet som utpekes til sertifiseringsorgan for kvalifiserte elektroniske signaturfremstillingssystemer.

9.2.2 Elektronisk tidsstempel

Elektronisk tidsstempel er i art. 3 nr. 33 definert som data i elektronisk form som knytter andre data i elektronisk form til et bestemt tidspunkt og dermed dokumenterer at sistnevnte data eksisterte på det gjeldende tidspunktet. I art. 42 fastsettes kravene til et kvalifisert elektronisk tidsstempel slik at de skal kunne knytte dato og tidspunkt til dataene på en slik måte at det med rimelighet utelukker muligheten for å endre dataene uten at dette oppdages. De kvalifiserte elektroniske tidsstemplene skal bygge på en presis tidskilde og være signert med den kvalifiserte tillitstjenestetilbyderens avanserte elektroniske signatur eller segl, eller med annen tilsvarende metode.

Europakommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenummer

på standarder om forbindelsen mellom data og tidspunkt for data og for bruk av nøyaktige tidskilder.

9.2.3 Elektronisk tjeneste for registrert sending

Elektronisk tjeneste for registrert sending er definert i artikkel 3 nr. 36 som en tjeneste som gjør det mulig å overføre data mellom tredjeparter elektronisk, og dokumenterer håndteringen av de overførte dataene, herunder dokumentasjon på sending og mottak av dataene, og som beskytter de overførte dataene mot tap, tyveri, skade og endring.

Kvalifiserte elektroniske tjenester for registrert sending skal blant annet oppfylle krav om at tjenesten tilbys av en kvalifisert tillitstjenestetilbyder, at tjenesten med høy grad av tillit sikrer avsenderens og mottakers identitet, og at forsendelsen eller mottakelsen av data er beskyttet av en kvalifisert tillitstjenestetilbyders avanserte elektroniske signatur eller segl på slik måte at det er umulig å endre dataene uten at dette oppdages, jf. art. 44.

Europakommisjonen kan fastsette referansenummer til standarder om forsendelse av data og prosesser for mottakelse av data.

9.2.4 Sertifikat for nettstedsautentisering

I henhold til artikkel 3 nr. 38 er et sertifikat for nettstedsautentisering en attestasjon som gjør det mulig å autentisere en nettside og knytte denne til den fysiske eller juridiske personen som sertifikatet er utstedt til. Tilbyder av kvalifiserte sertifikater for nettstedsautentisering skal oppfylle kravene som er å finne i vedlegg IV. For eksempel skal det angis at sertifikatet er utstedt som et kvalifisert sertifikat for nettstedsautentisering, det skal inneholde et sett data som entydig representerer den kvalifiserte tillitstjenestetilbyderen, herunder opplysninger om hvilken medlemsstat utstederen tilhører og den juridiske personens navn, og eventuelt organisasjonsnummer.

Europakommisjonen kan fastsette referanser til standarder for kvalifiserte sertifikater for nettstedsautentisering, hvor en ved oppfyllelse av standarden antas å oppfylle vedlegg IV.

9.3 Høringsinstansenes syn

Buypass anser ikke at høringsnotatet i tilstrekkelig grad tydeliggjør hva forordningen innebærer for tilbydere av ikke-kvalifiserte tillitstjenester og sertifikater. Videre mener Buypass at det bør presiseres at en tjenestetilbyder også kan sertifisere signaturfremstillingssystemet gjennom et sertifiseringsorgan i et annet medlemsland.

Datatilsynet viser til at tillitstjenestebegrepet er definert som elektroniske tjenester som normalt utføres mot betaling, og at regelverket synes å være beregnet på tjenester med et kommersielt aspekt. Dersom statlige deler av leveringstjenestene, eksempelvis Difis del av Sikker digital post, faller utenfor forordningens virkeområde, vil dette kunne utgjøre et lovtomt rom. Datatilsynet mener at det vil føre til en utilfredsstillende situasjon dersom disse tjenestene ikke omfattes av regelverket. Videre foreslår Datatilsynet at alle tilbydere av elektronisk postkasse bør pålegges å oppfylle kravene til kvalifisert tjenestetilbyder, da dette vil skape nødvendig tillit til tjenestene.

NAV og *Nkom* støtter departementets forslag om at Nasjonal sikkerhetsmyndighet v/SERTIT utpekes til sertifiseringsorgan. Hverken *Justis- og beredskapsdepartementet* eller *Nasjonal sikkerhetsmyndighet* anser at lovforslaget om gjennomføring av forordningen innebærer noen utvidelse av det ansvaret SERTIT allerede har, men påpeker at nye krav vil kunne medføre økt aktivitet for organet.

9.4 Departementets vurdering

Departementet viser til at det etter dagens esignaturlov kun er tilbydere av elektronisk signatur som er underlagt lovreguleringen. Med forordningen introduseres begrepet tillitstjenester, og dermed utvides hvem som er å anse som tilbyder og omfattes av lovreguleringen. At tillitstjenestebegrepet i art. 3 nr. 16 er definert som tjenester som normalt tilbys mot betaling, åpner etter departementets syn for at også ikke-kommersielle tjenester kan omfattes av forordningen. I motsetning til i esignaturloven omfattes også ikke-kvalifiserte tillitstjenestetilbydere av forordningen. I forordningens art. 19 pålegges disse for eksempel å gjennomføre sikkerhetsarbeid og iverksette tekniske og organisatoriske sikkerhetstiltak som står i forhold til den tjenesten som tilbys. Departementet antar at de fleste virksomheter forholder seg til krav om tilfredsstillende sikkerhet, for eksempel i kontrakter eller med utgangspunkt i forventninger fra markedet.

Departementet viser til forordningens fortale, hvor det fremgår at Kommisjonens gjennomgang av virkningene av esignaturdirektivet avdekket at

man ved kun å regulere elektronisk signatur ikke klarte å legge til rette for en digital samhandling internt i et land, eller på tvers av landegrensene. Dagens samfunn ønsker tilgjengelige digitale løsninger. Ved for eksempel inngåelse av en avtale vil partene i avtalen velge den metoden som oppleves sikrest og mest tilgjengelig. For å kunne sidestille elektroniske disposisjoner med tradisjonelle papirdisposisjoner er det etter departementets vurdering naturlig og viktig å utvide hvilke tjenester som omfattes av en lovregulering. Ved en slik utvidelse vil det bli stilt kvalitetskrav til tjenesten og til tilbydere av tjenesten, samt bli påsett at de lovbestemte kravene følges opp.

Som tidligere beskrevet stiller forordningen krav om sertifisering av kvalifiserte elektroniske signaturfremstillingssystemer i art. 30. Departementet tolker bestemmelsen slik at den ikke pålegger medlemslandene noen plikt til å tilby et slikt sertifiseringssystem. Den som skal tilby kvalifisert elektronisk signatur, kan velge å benytte seg av et signaturfremstillingssystem som er sertifisert i et annet medlemsland.

Europakommisjonen kan i henhold til art. 30 fastsette en delegert rettsakt med kriterier til det organet som utpekes som sertifiseringsorgan for kvalifiserte elektroniske signaturfremstillingssystemer. Innholdet i en slik rettsakt kan påvirke hvilken myndighet som anses best egnet til å foreta sertifiseringen.

Departementet viser til at det i Norge er Nasjonal sikkerhetsmyndighet v/SERTIT som innehar rollen som norsk sertifiseringsmyndighet etter ISO/IEC 15408 (dvs. Common Criteria) og deltar under de internasjonale avtalene CCRA og SOGIS MRA (europeisk) som kvalifisert sertifiseringsmyndighet på dette området. Etter departementets syn vil det derfor være naturlig at det er SERTIT som utpekes som sertifiseringsorgan etter artikkel 30, jf. art. 39 pkt. 2 i Norge, dersom man ser at det er behov for å ha et system for slik sertifisering i Norge.

I lovforslagets § 1 annet ledd er Kongen tillagt forskriftsfullmakt til å fastsette nærmere regler om krav til, og sertifisering av, kvalifiserte elektroniske signaturfremstillingssystemer.

10 Krav til tillitstjenestetilbyderne – samsvarsvurdering

10.1 Forslaget

I høringsnotatet presiserte departementet at tillit til at tjenestene er sikre og at de fungerer er en viktig forutsetning for at tillitstjenestene tas i bruk. Forordningen oppstiller flere og sterkere forpliktelser som tjenestetilbydere må forholde seg til, enn hva tilfellet er ved dagens lovregulering.

En tjenestetilbyder som ønsker å tilby en kvalifisert tillitstjeneste, må etter forordningens art. 21 underrette tilsynsmyndigheten om dette. Sammen med meldingen skal det foreligge en samsvarsrevisjonsrapport gjennomført av et godkjent samsvarsvurderingsorgan for å sjekke om tillitstjenestetilbyderen oppfyller forordningens krav. Tilsynsmyndigheten skal gjennomgå rapporten og på bakgrunn av denne avgjøre om tilbyderen av en tillitstjeneste kan anses som en kvalifisert tillitstjenestetilbyder. Først etter innvilgelsen av slik status, som markeres i tillitslisten, kan tilbyderen tilby sin kvalifiserte tillitstjeneste i markedet.

Europakommisjonen kan fastsette gjennomføringsrettsakter om formater og prosedyrer for notifisering av ny tjeneste til tilsynsmyndigheten.

Et samsvarsvurderingsorgan er i forordningens art. 3 nr. 18 definert som et organ som er definert i art. 2 nr. 13 i forordning (EF) nr. 765/2008, og som er akkreditert i overensstemmelse med den samme forordningen med kompetanse til å utføre samsvarsrevisjoner av en kvalifisert tillitstjenestetilbyder og de kvalifiserte tillitstjenestene som tilbys. Art. 2 nr. 13 omfatter organer som utfører samsvarsvurderingsvirksomhet, herunder kalibrering, overprøving, sertifisering og inspeksjon.

I henhold til art. 20 nr. 4 kan Europakommisjonen fastsette gjennomføringsrettsakter med referanser til standarder for akkreditering av samsvarsvurderingsorganer og samsvarsvurderingsrapporten, og for gjennomføringen av samsvarsvurderingen.

Etter art. 19 er tilbydere av tillitstjenester, både kvalifiserte og ikke-kvalifiserte, pålagt å gjennomføre sikkerhetsarbeid i virksomheten. Dette uttrykkes blant annet ved at de skal iverksette tekniske og organisatoriske sikkerhetstiltak som er proporsjonale med risikoen knyttet til den tjenesten de tilbyr. For å sikre transparens og oppnå tillit er tilbyderne også pålagt å melde fra til tilsynsmyndigheten og eventuelt andre myndigheter om uønskede sikkerhetshendelser. Rapporteringen skal gjøres så snart som mulig og senest innen 24 timer etter at den uønskede hendelsen er oppdaget.

Europakommisjonen kan fastsette gjennomføringsrettsakter som utdyper det sikkerhetsarbeidet tillitstjenestetilbydere er pålagt å gjennomføre, og om plikten til å rapportere om uønskede sikkerhetshendelser.

I henhold til art. 20 nr. 2 kan tilsynsmyndigheten gjennomføre tilsyn ved virksomheten, eller pålegge ny samsvarsrevisjon utenom den allerede fastsatte revisjonssyklusen. Ved uoverensstemmelse med forordningen og dersom den kvalifiserte tillitstjenestetilbyderen ikke iverksetter tiltak for å rette opp i dette, kan tilsynsmyndigheten vurdere å trekke tilbake kvalifisert status og markere dette i tillitslisten, jf. art. 22.

Etter art. 20 skal tilbydere av kvalifiserte tillitstjenester hvert andre år gjennomføre en samsvarsrevisjon for å sjekke at de krav som forordningen stiller, fortsatt oppfylles. Den kvalifiserte tillitstjenestetilbyderen skal selv dekke kostnadene forbundet med samsvarsrevisjonen, og sende rapporten for gjennomgang til tilsynsmyndigheten.

Artikkel 24 stiller krav til den kvalifiserte tillitstjenestetilbyderens identifikasjonskontroll, som skal gjennomføres ved hjelp av hensiktsmessige midler og i overensstemmelse med nasjonal rett for å sikre riktig identitet til sertifikatinnehaveren. Det stilles krav om fysisk oppmøte, slik som det også kreves etter dagens regulering i esignaturloven § 13, jf. forskrift om krav til utstedere av kvalifiserte sertifikater § 7. I tillegg tillater forordningen blant annet bruk av elektroniske identitetsbevis hvor personlig oppmøte har vært gjennomført, og som oppfyller kravene i forordningens artikkel 8 i forbindelse med sikringsnivåene «betydelig» og «høy».

10.2 Høringsinstansenes syn

NAV mener at det bør utarbeides nærmere kvalifikasjonskrav til selskaper som skal akkrediteres til å utføre samsvarsvurderinger.

Nkom mener at det vil være fordelaktig dersom det finnes revisjonsselskaper i Norge som akkrediteres av Norsk Akkreditering til å være samsvarsrevisjonsorgan etter forordningen.

10.3 Departementets vurdering

Et samsvarsvurderingsorgan er som tidligere nevnt et organ som er akkreditert i overensstemmelse med forordning (EF) nr. 765/2008 med kompetanse til å utføre samsvarsvurderinger av en kvalifisert tillitstjenestetilbyder og de kvalifiserte tillitstjenestene som tilbys. EØS-vareloven § 3 utpeker Norsk akkreditering som akkrediteringsorgan etter den nevnte forordningen, og det vil derfor være Norsk akkreditering som vil akkreditere eventuelle samsvarsvurderingsorganer i Norge.

Norsk akkreditering benytter ISO-standarder i akkrediteringen av samsvarsvurderingsorganer. Departementet legger herunder til grunn at Norsk akkreditering er nærmest til å vurdere hvilke ISO-standarder det er aktuelt å benytte i forbindelse med akkrediteringen av selskaper som ønsker å foreta samsvarsvurderinger av tjenestetilbydere. Det vises til at Kommisjonen per dags dato ikke har besluttet hvilke standarder som skal brukes, og det er derfor naturlig at Norsk akkreditering benytter tilsvarende standarder som andre europeiske akkrediteringsorganer. Lovforslaget § 1 andre ledd gir Kongen adgang til å gi forskrift om akkreditering av samsvarsvurderingsorganer, utforming av samsvarsrevisjonsrapport og regler for gjennomføring av samsvarsrevisjoner mv. Departementet antar at det vil kunne bli aktuelt å benytte denne forskriftshjemmelen dersom det konstateres avvik mellom standardene de ulike akkrediteringsorganene legger til grunn, og norsk næringsliv berøres av dette.

I henhold til EØS-vareloven skal Norsk akkreditering føre tilsyn med de samsvarsvurderingsorganene som det har utstedt akkrediteringsbevis til, jf. lovens § 2 og forordning (EF) nr. 765/2008 art. 5 nr. 3. Betaling for akkrediteringstjenestene er fastsatt i forskrift 1. juli 2013 nr. 821 om gebyrer for Norsk akkrediterings tjenester. Dersom et akkreditert samsvarsvurderingsorgan ikke lenger er kompetent til å utøve samsvarsvurderingsvirksomheten, eller det på en alvorlig måte har unnlatt å oppfylle sine forpliktelser, skal akkrediteringsorganet treffe «alle egnede tiltak for å begrense, midlertidig oppheve eller trekke tilbake akkrediteringsbeviset», jf. samme forordning art. 5 nr. 4.

Det foreligger ingen forpliktelse for medlemslandene til å ha et nasjonalt samsvarsrevisjonsorgan. En tjenestetilbyder vil også kunne benytte et akkreditert samsvarsvurderingsorgan fra et annet medlemsland. Det kan være en fordel dersom det finnes revisjonsselskaper i Norge som blir akkreditert til å være samsvarsvurderingsorganer, sett i lys av nasjonale organers verdifulle kunnskaper om lokale forhold. Departementet mener imidlertid at det må være opp til potensielle aktører selv å vurdere om de anser det å være revisjonsselskap som en tilstrekkelig markedsmulighet til å ønske å bli akkreditert. Departementet mener at det ikke er naturlig at dette blir en statlig oppgave. Det eksisterer et europeisk marked, og norske bedrifter kan benytte seg av samsvarsrevisjonsorganer etablert i EU.

11 Tillitsliste

11.1 Forslaget

Det ble i høringsnotatet redegjort for forordningens artikkel 22, som pålegger medlemslandene å lage, vedlikeholde og publisere en tillitsliste med informasjon om de kvalifiserte tillitstjenestetilbyderne og deres kvalifiserte tillitstjenester. Medlemslandene skal notifisere til Kommisjonen det myndighetsorganet som er ansvarlig for tillitslisten.

En tillitsliste er allerede etablert gjennom Europaparlaments- og rådsdirektiv 2006/123/EC om tjenester i det indre markedet (tjenestedirektivet) artikkel 8, gjennomført ved Kommisjonsbeslutning 2009/767/EF. Medlemslandene er i henhold til disse bestemmelsene pålagt å etablere, vedlikeholde og publisere en tillitsliste med oversikt over utstedere av kvalifiserte sertifikater underlagt tilsyn. Under dagens ordning er det Nkom som er ansvarlig for tillitslisten.

For å kunne ha en oppdatert og riktig tillitsliste kan det være nødvendig å pålegge tillitstjenestetilbyderne å bidra. Av denne grunn foreslo departementet i høringsnotatet at Kongen kan fastsette forskrift for tillitslisten, jf. § 1, andre ledd i lovforslaget. Kommisjonens gjennomføringsbeslutning (EU) 2015/1505 av 8. september 2015 gir nærmere krav til tekniske spesifikasjoner og formater for tillitslisten i henhold til artikkel 22(5). Denne vil gjennomføres som forskrift til loven.

Videre ble det i høringsnotatet foreslått at tilsynsmyndigheten bør være ansvarlig myndighet for oppfyllelse av forpliktelsene etter art. 22 i forordningen.

11.2 Høringsinstansenes syn

Universitetet i Oslo er skeptisk til at tilsynsmyndigheten også skal ha ansvar for tillitslisten, da dette etter deres oppfatning kan medføre en uheldig sammenblanding av roller. De mener at ansvaret for tillitslisten bør legges til et annet organ, og foreslår Difi.

11.3 Departementets vurdering

Tillitslisten skal benyttes aktivt til å markere status for utstederne av tillitstjenester. Departementet mener at det er tilsynsmyndigheten som vil være nærmest tillitstjenestetilbyderne til å gjøre dette. Det er også tilsynsmyndigheten som vil kunne trekke tilbake kvalifisert status hos en tilbyder, dersom dette viser seg nødvendig. Videre er det tilsynsorganet som skal gjennomgå samsvarsrevisjonsrapportene for å vurdere hvorvidt forordningens krav er oppfylt. Departementet anser det derfor som naturlig at det er tilsynsorganet som også er ansvarlig for tillitslisten.

Departementet kan ikke se at tilsynsoppgavene vil være i konflikt med rollen som ansvarlig for tillitslisten. Det bemerkes at tillitslisten er en oversikt over tilbydere av kvalifiserte tjenester, og at oppgavene som tilligger den ansvarlige for listen, langt på vei kan karakteriseres som en formalkontroll. Hvorvidt en tilbyder kommer på listen eller ei, avhenger av om tilbyderen oppfyller forordningens krav til kvalifiserte tilbydere av tillitstjenester, og departementet anser det derfor ikke som problematisk at tilsynsorganet også har ansvar for tillitslisten.

Departementet opprettholder forslaget slik det kommer til uttrykk i høringsnotatet, og legger til grunn at tilsynsorganet bør være ansvarlig myndighet for oppfyllelse av forpliktelsene etter art. 22.

12 Rettsvirkning av kvalifiserte elektroniske tillitstjenester, signaturer og segl

12.1 Forslaget

Artikkel 25 regulerer rettsvirkninger av elektroniske signaturer. Liknende bestemmelser gis for elektroniske segl (art. 35), elektronisk tidsstempel (art. 41), elektronisk tjeneste for registrert sending (art. 43) og elektroniske dokumenter (art. 46).

Det følger av art. 25 nr. 1 at en elektronisk signatur ikke må nektes rettsvirkning og anerkjennelse som bevis under rettssaker alene på grunn av at den er i elektronisk form, eller at den ikke oppfyller kravene til kvalifiserte elektroniske signaturer. Tilsvarende regler finnes om elektroniske segl (35.1), elektronisk tidsstempling (41.1) og elektronisk tjeneste for registrert sending i henhold til art. 43 pkt. 1. Etter art. 25 nr. 2 skal en kvalifisert elektronisk signatur ha samme rettsvirkning som en håndskreven underskrift.

I forordningen art. 35 nr. 2 fastsettes det at for et kvalifisert elektronisk segl gjelder det en presumpsjon for integriteten (uforandrethet) og nøyaktigheten av opprinnelsen av de data som det kvalifiserte elektroniske seglet er knyttet til. Tilsvarende presumpsjonsbestemmelser finnes i art. 41 nr. 2 og 43 nr. 2 om hhv. kvalifisert elektronisk tidsstempel og kvalifisert elektronisk tjeneste for registrert sending.

Etter art. 25. nr. 3 skal en kvalifisert elektronisk signatur som er basert på et kvalifisert sertifikat og utstedt i en medlemsstat, anerkjennes som en kvalifisert elektronisk signatur i alle andre medlemsstater.

Artikkel 27 regulerer bruk av avanserte signaturer i offentlige tjenester. Dersom en medlemsstat krever bruk av avansert elektronisk signatur, herunder avansert elektronisk signatur basert på et kvalifisert sertifikat, for bruk av elektroniske tjenester hos et offentlig organ, så skal medlemsstaten også anerkjenne tilsvarende signaturer i nærmere angitte referanseformater og referansemetoder. Kommisjonen har i gjennomføringsrettsakt 2015/1506 fastsatt at tre signaturformater må anerkjennes (XAdES, CAdES, PAdES, som er avanserte elektroniske signaturer i formatene XML, CMS og PDF). Videre skal andre formater anerkjennes forutsatt at tillitstjenestetilbyderens hjemland tilbyr en gratis valideringstjeneste som oppfyller nærmere angitte krav, jf. gjennomføringsrettsaktens art. 2. Medlemsstatene kan ikke kreve bruk av elektronisk signatur på et høyere sikkerhetsnivå enn kvalifisert elektronisk signatur for grenseoverskridende bruk av elektroniske tjenester som tilbys av et offentlig organ, jf. forordningens art. 27 nr. 3.

Tilsvarende bestemmelser gjelder for elektroniske segl, jf. art. 37.

12.2 Høringsinstansenes syn

Brønnøysundregistrene, *Buypass*, *Direktoratet for e-helse*, *Forbrukerombudet* og *POD* er enige med departementet i at forskriftskompetansen som gis i esignaturloven § 5, i all hovedsak er dekket av forvaltningsloven § 15a, og at det sannsynligvis ikke er behov for annet enn mindre justeringer av ordlyden i sistnevnte bestemmelse når esignaturloven oppheves. *Direktoratet for e-helse* påpeker videre betydningen av at eforvaltningsforskriften og kravspesifikasjon for PKI i offentlig sektor ses i sammenheng med forordningen, og at alle krav som stilles i Norge, er i henhold til forordningens formål.

Datatilsynet mener at det bør inntas en hjemmel for forskriftskompetanse for regulering av den statlige delen av de elektroniske leveringstjenestene for å sikre en forsvarlig regulering med hensyn til ansvar og sikkerhet.

12.3 Departementets vurdering

Avtalefrihet, herunder formfrihet, er et sentralt prinsipp i norsk rett. Som utgangspunkt velger partene selv i hvilken form de ønsker å inngå en bindende avtale, for eksempel muntlig, skriftlig på papir eller elektronisk. I forbindelse med vedtakel-

sen av esignaturloven valgte man å ta inn en presisering om at en kvalifisert elektronisk signatur alltid vil oppfylle et krav om underskrift, forutsatt at disposisjonen kan gjennomføres elektronisk, jf. Ot.prp. nr. 82 (1999–2000) s. 36 flg.

Etter departementets syn er derfor regelen i art. 25 nr. 1 og 2 om rettsvirkninger i tråd med norsk rett. Departementet legger til grunn at det fortsatt gjelder en forutsetning om at disposisjonen kan gjennomføres elektronisk, og viser til avgrensningen i artikkel 2 nr. 3 mot rettslige og prosessuelle forpliktelser som gjelder formkrav. Det er således ikke noe rettslig i veien for at elektroniske dokumenter (jf. forordningens art. 46) legges frem som bevis for en norsk domstol, uten signatur eller med elektronisk signatur (jf. forordningen art. 25 nr. 1) eller elektronisk segl (jf. forordningen art. 35 nr. 1).

Norsk sivilprosess bygger på prinsippet om fri bevisføring og fri bevisvurdering, jf. lov 17. juni 2005 nr. 90 om mekling og rettergang i sivile tvister (tvisteloven) §§ 21-2 og 21-3. Dette innebærer at partene i utgangspunktet kan føre ethvert bevis de finner hensiktsmessig, og at dommeren etter en samvittighetsfull prøvelse av hele saken avgjør hvilket faktum som ut fra en sannsynlighetsvurdering skal legges til grunn. Det er således ikke noe rettslig i veien for at elektroniske dokumenter legges frem som bevis for en norsk domstol, jf. forordningens art. 25 nr. 1 og de tilsvarende bestemmelsene om elektronisk segl, tidsstempling og elektronisk tjeneste for registrert sending.

Nettopp grunnet de nevnte prinsippene om avtalefrihet, fri bevisføring og fri bevisvurdering representerer ikke forordningens bestemmelser om den juridisk bindende virkningen av elektroniske signaturer og elektroniske dokumenter utfordringer for Norge. I motsetning til i en rekke europeiske land har det lenge vært en etablert oppfatning i norsk rett at det ikke er grunnlag for å nekte et dokument rettslig virkning bare fordi det er elektronisk. I nyere tid er det dessuten foreslått flere lovendringer som formelt sidestiller elektronisk dokumentasjon med dokumentasjon utstedt på papir, eksempelvis Prop. 6 L (2016–2017), som introduserer bestemmelser om teknologinøytralitet i tinglysingsloven, inkassoloven og tvangsfullbyrdelsesloven.

Bestemmelsene om presumpsjon for integritet og om korrekt opphav for kvalifisert elektronisk segl (jf. forordningen art 25 nr. 2), for korrekt tidspunkt og integritet for kvalifisert elektronisk tidsstempel (jf. forordningen art. 41 nr. 2) og for integritet og korrekt tidspunkt for sending og mottak for elektronisk rekommandert sending (jf. forordningen art. 43 nr. 2 kan sies å gripe inn i dommerens vekting av bevisene i en rettssak. Etter departementets syn går disse bestemmelsene likevel ikke lengre enn hvordan man må anta at slike data uansett hadde blitt vurdert. De tekniske metodene som bestemmelsene gjelder, må i utgangspunktet antas å ha høy bevisverdi. Bestemmelsene er heller ikke til hinder for at motbevis føres.

Bruk av elektronisk signatur i offentlig sektor

Forordningens krav til anerkjennelse av signaturer i referanseformater mv. vil bidra til at private kan gjenbruke sin signeringsløsning ved bruk av offentlige tjenester i ulike medlemsstater, og kan således bidra til å stimulere tilbudet av slike løsninger. For forvaltningen innebærer forordningen at det i forbindelse med etablering av krav om bruk av elektronisk signering må tas høyde for at signaturen kan komme inn i andre formater enn det formatet forvaltningen foretrekker, jf. gjennomføringsrettsaktens bestemmelser.

Departementet legger til grunn at forordningen bare gjelder anerkjennelsen av signaturens evne til å oppfylle eventuelle formkrav til selve signaturen, men at det ikke innebærer at ethvert signert dokument vil oppfylle alle formkrav på det aktuelle rettsområdet. Formkrav om bruk av signatur kan eksempelvis være begrunnet i at signaturen skal sannsynliggjøre at dokumentet har et bestemt opphav og et bestemt innhold. I den grad det er stilt andre krav til dokumentet eller innsendingsmåten, som at data skal sendes i et elektronisk og strukturert format, vil dette måtte vurderes for seg. Slike krav kan de facto få betydning for hvilke signaturformater som i praksis kan benyttes, ettersom signaturformatene kan ha ulik evne til å understøtte slike krav.

Norsk forvaltning stiller i dag i liten grad krav til bruk av avanserte elektroniske signaturer eller segl. I stor grad benyttes elektroniske nettløsninger som baserer seg på autentisering av aktørene, uten digital signering av dokumenter. For de løsninger som krever bruk av avanserte signaturer, vil forordningen kunne innebære behov for noen tilpasninger for å etterleve anerkjennelsesplikten. Hvor store tilpasninger som kreves, vil blant annet bero på i hvor stor grad andre signaturformater enn referanseformatene vil bli brukt og hvordan de tilhørende valideringstjenester i så fall vil utformes.

Esignaturloven § 5 inneholder hjemmel til å fastsette nærmere regler om hvilke krav som skal stilles til kvalifiserte elektroniske signaturer som skal brukes ved kommunikasjon med og i offent-

lig sektor. Eforvaltningsforskriften er i dag hjemlet i både forvaltningsloven § 15a og esignaturloven § 5. Etter departementets vurdering er forskriftskompetansen som gis i esignaturloven, i all hovedsak dekket av forvaltningsloven § 15a. For forvaltningsorganer som er regulert i særlov, vil forvaltningsloven ikke gjelde. Det er derfor behov for å videreføre hjemmelen i esignaturloven til ny lov. Departementet foreslår en justering av innholdet for å harmonisere den med ordlyden i fvl. § 15a.

13 Tilsynsorganet

13.1 Forslaget

Tilsynsmyndighetene skal gjennomføre tilsynsaktiviteter i forkant av utstedelse av en kvalifisert tillitstjeneste og ved kontroller i ettertid, for å påse at forordningen oppfylles. Tydeliggjøringen av tilsynets oppgaver og roller slik de fremkommer i art. 17 bidrar til at alle tilsynsmyndigheter, uavhengig av land de er etablert i, skal gjennomføre de samme oppgavene.

For å kunne foreta et godt og grundig tilsyn med en velbegrunnet konklusjon er tilsynsmyndigheten avhengig av å kunne få tilgang til de nødvendige dokumenter om tjenestetilbyderens virksomhet. Det kan også være nødvendig å foreta kontroller i virksomhetens lokaler i forbindelse med tilsynet. Esignaturloven § 17 gir tilsynsmyndigheten tilgang til dokumenter og rett til å kreve adgang til virksomhetens lokaler. I høringsnotatet uttalte departementet at det er viktig å videreføre disse beføyelsene i den nye loven slik at tilsynet skal kunne gjennomføres i samsvar med forordningens formål. Bestemmelser om dette fremkommer i lovforslagets § 4.

Departementet foreslo videre at tilsynsmyndigheten skal kunne gi påbud om at forhold som er i strid med bestemmelser etter loven skal opphøre og stille vilkår for oppfyllelse, jf. lovforslagets § 3. Som etter gjeldende rett foreslo departementet at tilsynets enkeltvedtak skal kunne påklages, jf. lovforslagets § 6.

Som tidligere omtalt foreslo departementet også at tilsynsmyndigheten skal være ansvarlig myndighet til å føre en tillitsliste med informasjon om de kvalifiserte tillitstjenestetilbyderne og deres kvalifiserte tillitstjenester, jf. art. 22 i forordningen.

Nkom er utpekt som tilsynsmyndighet etter gjeldende rett. Med den nye forordningen er det flere typer tillitstjenester som reguleres og flere forpliktelser som påhviler både tjenestetilbyderne og tilsynsorganene. Departementet anså det derfor som naturlig å vurdere om Nkom fortsatt bør være tilsynsorgan for denne typen tjenester, eller om det er andre myndigheter som burde ha oppgaven.

13.2 Høringsinstansenes syn

Hva gjelder spørsmålet om tilsynsmyndighet, støtter *BankID, Brønnøysundregistrene, Buypass, Commfides, Datatilsynet, Finans Norge, Justis- og beredskapsdepartementet, Nasjonal Sikkerhetsmyndighet, NAV, Nkom* og *Samferdselsdepartementet* forslaget om at Nkom oppnevnes som tilsynsorgan etter den nye loven. *Justis- og beredskapsdepartementet* uttaler at Nasjonal Sikkerhetsmyndighet (NSM) kunne ha vært en egnet kandidat som tilsynsmyndighet, men da sistnevnte er foreslått som sertifiseringsorgan, er det naturlig å legge tilsynsoppgavene til Nkom.

Direktoratet for e-helse anbefaler at departementet i tillegg til Nkom også vurderer NSM og Datatilsynet før det tas en endelig beslutning.

Etter *POD*s oppfatning er både Nkom og NSM aktuelle som tilsynsmyndighet. *POD* fremholder at kravene til tilsynsorganets kompetanse og omfang vil bli vesentlig mer omfattende ved innføringen av forordningen, og at det vil kreve betydelige ressurser dersom Nkom alene skal bygge opp og vedlikeholde tilstrekkelig kompetanse. *POD* viser til forordningens artikkel 18 om tilsynsorganenes samarbeid over landegrenser, og anser det som hensiktsmessig at det etableres et nordisk samarbeid for å dra nytte av hverandres kompetanse. *POD* ønsker ikke å konkludere med hensyn til valg av tilsynsorgan, men ber om at det tas med i vurderingen hvordan NSMs kompetanse kan utnyttes for oppgaver knyttet til tilsyn i lys av det økte omfanget. *Universitetet i Oslo* mener at tilsynsmyndigheten ikke også bør ha ansvar for tillitslisten, og trekker frem Difi som et alternativ.

13.3 Departementets vurdering

Nkom driver tilsyn med tilbydere av posttjenester og med tilbydere av elektronisk kommunikasjonsnett og -tjenester etter lov om formidling av landsdekkende postsendinger (postloven) og lov om elektronisk kommunikasjon (ekomloven). Nkom har som oppgave å sikre brukerne i hele landet gode, rimelige og fremtidsrettede elektroniske

kommunikasjonstjenester og posttjenester. Nkom har vært tilsynsmyndighet etter esignaturloven siden loven ble innført i 2001. Av forarbeidene fremgår det at Nkom ble valgt som tilsynsmyndighet blant annet fordi etaten allerede hadde ansvar for å føre tilsyn med aktørene på post- og teleområdet, og på grunn av sin kompetanse på det tekniske, økonomiske og juridiske området, jf. Ot.prp. nr. 82 (1999–2000) pkt. 8.7.3 flg. I ettertid har Nkom også fått i oppgave å føre en liste over tjenestetilbydere med hjemmel i tjenesteloven, som nå skal utvides gjennom forordningen.

Departementet har vurdert om det er andre myndigheter som kan være aktuelle som tilsynsmyndighet, herunder NSM, Datatilsynet og Difi.

NSM er nasjonal varslings- og koordineringsinstans for alvorlige dataangrep og andre IKT-relaterte sikkerhetshendelser, og fører tilsyn med at sikkerhetslovens bestemmelser om forebyggende sikkerhetstjeneste etterleves. Departementet vurderer NSM som en egnet kandidat til rollen som tilsynsorgan etter forordningen. Imidlertid finner departementet det naturlig at NSM ved SERTIT utpekes som sertifiseringsorgan. SERTIT er opprettet som sertifiseringsorgan for IT-sikkerhet i Norge. SERTIT representerer også Norge i det internasjonale forumet «Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security (CCRA)». Oppgaven til et sertifiseringsorgan er å forestå sertifisering av IT-produkter og systemer.

Departementet anser det i utgangspunktet som mest hensiktsmessig at sertifiseringsorganet og tilsynsorganet ikke er den samme myndigheten, fordi organene har noe ulike roller og oppgavene baserer seg på ulike regelverk. Mens sertifiseringsorganet skal sertifisere at kvalifiserte signaturframstillingssystemer oppfyller sikkerhetskrav i henhold til tekniske standarder, er tilsynsmyndigheten pålagt de tilsynsoppgavene som er skissert i art. 17. Gjennomføring av sertifisering og tilsyn stiller for øvrig også ulike krav til kompetanse hos personell som skal gjennomføre oppgavene. Det styrker dessuten tilliten til tilsynsaktiviteten etter art. 17 at tilsynet ikke har hatt noen rolle i sertifiseringen av produkter og systemer, da dette betyr at to uavhengige parter har vurdert oppfyllelse av sikkerhetskrav. Departementets vurdering er således at selv om NSM besitter kompetanse som kan utnyttes i forbindelse med tilsynsoppgavene etter forordningen, er det mer hensiktsmessig at forordningens oppgaver knyttet til henholdsvis sertifisering og tilsyn legges til to ulike organer. Det er også slik de fleste europeiske land har innrettet seg.

Datatilsynet har som hovedmål å bidra til at personvernlovgivningen etterleves og at alle skal ha beskyttelse i tråd med gjeldende personopplysningsregelverk. I kraft av sine roller som både tilsyn og ombud fører Datatilsynet kontroll med personvernregelverket og arbeider for å forhindre misbruk av personopplysninger. Datatilsynet har på denne bakgrunn for eksempel erfaring med vurdering av hvorvidt sikkerhetsbrudd tilsier at enkeltpersoner skal informeres. Tilsynsoppgavene etter forordningen ligger i utgangspunktet utenfor kjernen av Datatilsynets virksomhet. Departementet vurderer derfor ikke Datatilsynet som den mest aktuelle kandidaten til å være tilsynsorgan.

Som forvalter av ID-porten og Kravspesifikasjonen for PKI i offentlig sektor har Difi god faglig kompetanse på området. Difi har imidlertid ikke erfaring med tilsynsvirksomhet, som er en kompetanse det vil ta tid å bygge opp. Det kan også oppstå en uheldig dobbeltrolle som følge av oppgavene knyttet til regelverksforvaltning og forhandlingen med eID-leverandørene i ID-porten.

Etter departementets vurdering taler den erfaringen og ekspertisen Nkom har på teleområdet generelt, og som tilsynsmyndighet etter gjeldende esignaturlov spesielt, for å utpeke Nkom som tilsynsmyndighet også etter den nye loven. Langt på vei de fleste høringsinstansene støtter dette, og flere trekker frem at Nkom har etablert et godt samarbeid med aktørene i bransjen som det vil være nyttig å bygge videre på når det utvidete tilsynet skal etableres. På bakgrunn av dette fastholder departementet forslaget om at Nkom oppnevnes som tilsynsorgan etter den nye loven.

14 Erstatningsansvar og bevisbyrde

14.1 Forslaget

I art. 13 i forordningen gis det bestemmelser om erstatning. En tillitstjenestetilbyder er erstatningsansvarlig for skade som forsettlig eller uaktsomt påføres en fysisk eller juridisk person som følge av manglende oppfyllelse av forordningens forpliktelser.

Det er ulik bevisbyrderegel for den kvalifiserte tillitstjenestetilbyderen og den ikke-kvalifiserte tillitstjenestetilbyderen. For den ikke-kvalifiserte tillitstjenestetilbyderen er det den skadelidte som må bevise at tillitstjenestetilbyderen har handlet forsettlig eller uaktsomt. Den kvalifiserte tillitstjenestetilbyderen antas å ha handlet forsettlig eller uaktsomt med mindre den kvalifiserte tillitstjenestetilbyderen beviser at skaden oppstod uten forsett eller uaktsomhet fra tillitstjenestetilbyderens side. Dette er en videreføring av erstatningskravet etter esignaturloven. Begrunnelsen for omvendt bevisbyrde for kvalifiserte tjenestetilbydere er å styrke mottakerens tillit til kvalifiserte sertifikater.

I art. 13 pkt. 2 innskrenkes erstatningsansvaret for tillitstjenestetilbydere. Dersom tillitstjenestetilbyderen gir grundig informasjon til sine kunder om begrensningene i bruken av tjenestene, og disse begrensningene er identifiserbare for kundene, bortfaller erstatningsansvaret for skader som påføres ved at bruken av tjenesten går ut over de begrensninger som ligger i den.

14.2 Høringsinstansenes syn

Difi foreslår at det i lovforslaget § 1 bør tas inn en forskriftshjemmel som gjør det mulig å fastsette et minstebeløp for erstatningsansvaret for eID-leverandører som benyttes i offentlig sektor. *Difi* viser til at det i ID-porten per i dag benyttes eID-leverandører som har erstatningsansvar på minst 5000 kroner, blant annet ved brudd på plikter i forbindelse med utstedelse av eID.

14.3 Departementets vurdering

Artikkel 13 skal anvendes i overensstemmelse med nasjonale regler om erstatningsansvar. Dette utdypes i fortalens pkt. 37, hvor det fremkommer at forordningen ikke skal påvirke nasjonale bestemmelser om definisjonen av skade, forsett, uaktsomhet eller relevante prosedyreregler. Departementet anser derfor at det ikke foreligger behov for egne nasjonale regler som behandler erstatning etter forhold regulert i forordningen. Også etter gjeldende lov er det omvendt bevisbyrde for utstedere av kvalifiserte sertifikater, jf. esignaturloven § 22 andre ledd.

Departementet foreslår at lovforslaget § 1 inkluderer adgang til å forskriftsregulere et minstekrav til erstatningsansvar for eID-er som skal benyttes i offentlig sektor.

15 Sanksjoner og straff

15.1 Forslaget

Etter forordningen art. 16 er det medlemsstatene som fastsetter sanksjoner for overtredelse av forordningen. Sanksjonene skal være effektive, stå i rimelig forhold til overtredelsen og ha avskrekkende virkning.

Esignaturloven inneholder bestemmelser om både tvangsmulkt og straffansvar for en sertifikatutsteder. Som nevnt i høringsnotatet har bestemmelsene etter hva departementet kjenner til, hittil ikke vært brukt, og aktørene i bransjen har vært opptatt av gode skussmål. Departementet stilte derfor spørsmål ved om bestemmelsene burde videreføres. Loven vil omfatte en rekke nye typer tillitstjenester som hittil ikke har vært særskilt regulert, der en tjenestetilbyder pålegges flere plikter.

Tilsynsmyndigheten har imidlertid allerede en rekke beføyelser som kan iverksettes ved brudd på pliktene, jf. pkt. 13.1. Når det gjelder brudd på bestemmelsene om personopplysninger, dekkes disse av den generelle straffebestemmelsen i personopplysningsloven § 48. Departementet antok også at enkelte tilfeller vil omfattes av markedsføringslovens sanksjonsbestemmelser, for eksempel utstedelse av kvalifiserte tillitstjenester som i virkeligheten ikke er kvalifiserte.

Det ble i høringsnotatet argumentert for at preventive hensyn og hensynet til en effektiv håndheving likevel taler for at dagens straffebestemmelse og adgangen til å ilegge tvangsmulkt bør videreføres. De forpliktelsene som forordningen pålegger utstederne av tillitstjenester, er med på å ivareta viktige offentlige eller private interesser, og brudd på pliktene kan få alvorlige konsekvenser for dem som rammes. Ved at forordningen innfører regler om flere typer tillitstjenester, er det sannsynlig at det vil oppstå et nytt marked. En straffebestemmelse kan virke preventivt mot useriøse aktører. Departementet anså at det kan være grunnlag for å begrense bestemmelsene til å omfatte utstedere av *kvalifiserte* tillitstjenester, da det ved bruk av slike tjenester er et spesielt behov for tillit.

15.2 Høringsinstansenes syn

Nkom anser det som mest hensiktsmessig at tilsynsorganet også bør kunne ilegge tvangsmulkt ved tilfeller av alvorlige overtredelser hos ikke-kvalifiserte tjenestetilbydere som ikke etterkommer påbud om retting. *Nkom* påpeker at det fremstår som uklart hvordan tilsynet skal kunne gripe inn overfor ikke-kvalifiserte tilbydere dersom sanksjonsbestemmelsene begrenses til å gjelde kvalifiserte tilbydere. *Norges teknisk-naturvitenskapelige universitet* mener at lovforslaget også bør inkludere en bestemmelse om straffansvar for forsettlige eller uaktsomme overtredelser som fører til identitetstyveri, identitetssvindel mv.

15.3 Departementets vurdering

Som etter gjeldende rett foreslår departementet at tvangsmulkt skal kunne anvendes for å sikre at bestemmelser som er gitt i eller i medhold av loven, overholdes. Mulkten skal ikke løpe før klagefristen er ute, og ved klage løper ingen tvangsmulkt før klagesaken er avgjort, med mindre klageorganet bestemmer noe annet. I tråd med gjeldende rett må mulktens størrelse fastsettes i lys av alminnelige forvaltningsrettslige prinsipper, herunder hensynet til rimelig forholdsmessighet mellom det målet som søkes oppnådd og de virkemidlene som benyttes, jf. Ot.prp. nr. 82 (1999–2000) s. 55.

Departementet ser at det kan være grunn til å gi tilsynsorganet adgang til også å ilegge tvangsmulkt ved tilfeller av alvorlige overtredelser hos ikke-kvalifiserte tjenestetilbydere. Imidlertid vurderer departementet at behovet for sanksjonsmidler er mest påtakelig i tilknytning til de kvalifiserte tillitstjenestene, da disse normalt benyttes til transaksjoner av stor betydning for brukerne, slik at bevaring av tillit må anses å være ekstra viktig. Dersom det etter regelverkets ikrafttredelse skulle oppstå et behov for å utvide adgangen til å ilegge tvangsmulkt til også å gjelde ovenfor ikke-kvalifiserte tilbydere, vil departementet vurdere dette nærmere.

Når det gjelder straff, må loven presisere nærmere hvilke bestemmelser som kan håndheves med dette, jf. Grunnloven § 96 om at straff krever hjemmel i formell lov. De forpliktelser som følger av forordningen er av ulik karakter og har ulik presisjonsgrad, jf. eksempelvis sikkerhetskravene i art. 19 nr. 1. Departementet har vektlagt at det må fremgå klart og tydelig hvilke handlinger som kan medføre straff. På denne bakgrunn foreslår departementet at straff kan idømmes den som forsettlig eller grovt uaktsomt:

a. opptrer som utsteder av kvalifisert tillitstjeneste uten å være registrert som dette etter loven
b. unnlater å gi opplysninger etter § 3
c. gir uriktige eller villedende opplysninger til tilsynet.

16 Avgift

16.1 Forslaget

Som nevnt i pkt. 9.1 gir esignaturloven § 24 hjemmel for å fastsette at registreringspliktige utstedere skal betale gebyr til tilsynet, og at gebyrene ikke må overstige kostnadene ved tilsynets virksomhet.

I forordningen utvides tilsynets oppgaver, både med hensyn til tilsynsobjekter og tilsynsoppgaver. Departementet foreslo i høringsnotatet at tilsynet fortsatt skal finansiere sin tilsynsvirksomhet gjennom gebyrer fra dem som omfattes av regelverket, og at nærmere retningslinjer fastsettes i forskrift.

16.2 Høringsinstansenes syn

Buypass poengterer at forordningen introduserer en rekke nye tillitstjenester og at arbeidsomfanget for myndigheten vil kunne variere fra tjeneste til tjeneste, slik at det er behov for å definere nærmere hvilke tilsynsoppgaver myndigheten skal ivareta. *Commfides* uttaler at kostnadene knyttet til tilsynsordningen må gjøres mer forutsigbare enn per i dag, og at en eventuell økning vil favorisere utenlandske tjenestetilbydere. *POD* mener det bør utarbeides en modell for gebyrberegning, slik at gebyrene som belastes tjenestetilbyderne, ikke blir for høye.

Nkom er enig i departementets forslag om å gjennomgå gebyrpraksisen for å oppdatere den i henhold til nytt regelverk. Videre bemerker *Nkom* at også ikke-kvalifiserte tjenestetilbydere bør være avgiftspliktige dersom det senere viser seg at tilsynet får mange oppgaver knyttet til oppfølging av disse tilbyderne.

Både *Nkom* og *Samferdselsdepartementet* ber med henvisning til Finansdepartementets retningslinjer for gebyr- og avgiftsfinansiering om at begrepet «gebyr» i lovforslagets § 7 endres til «avgift».

16.3 Departementets vurdering

Departementet legger til grunn at finansiering av tilsynsvirksomheten fastsettes i tråd med Finansdepartementets retningslinjer for gebyr- og avgiftsfinansiering av statlige myndighetshandlinger (R-112/2006 og R-4/2006), inkludert at finansieringen gjennomføres som avgift og ikke gebyr. Departementet legger videre til grunn at avgiften skal dekke, men ikke overstige, kostnadene ved tilsynets virksomhet etter forordningen, basert på kostnadseffektiv drift. Selve avgiftsfastsettelsen bør utformes slik at kostnaden blir så forutberegnelig som mulig for aktørene.

Samferdselsdepartementet er ansvarlig for gjeldende gebyrforskrift for Nkom. Forutsatt at Nkom blir tilsynsmyndighet etter den nye loven, er det naturlig at kompetansen til å fastsette forskrifter etter lovforslagets § 7 delegeres til Samferdselsdepartementet.

17 Lovteknisk gjennomføring

I EU gjelder forordninger som overnasjonale lover i den enkelte medlemsstat i kraft av å være vedtatt av de kompetente EU-organene. Siden EØS-avtalen ikke innebærer overføring av lovgivningsmyndighet til fellesskapsorganene, må regelverket gjennomføres i nasjonal rett. Det følger av artikkel 7 bokstav a i EØS-avtalen at en forordning som er EØS-relevant, skal gjøres til en del av den interne rettsordenen. En slik gjennomføring bør som hovedregel skje ved inkorporasjon. Inkorporasjon innebærer at det vedtas en lov- eller forskriftsregel som fastsetter at forordningen i EØS-tilpasset form skal gjelde direkte i norsk rett. Forordninger kan unntaksvis bli gjennomført ved transformasjon, som innebærer at det vedtas en lov eller forskrift som i mer eller mindre bearbeidet form gjengir bestemmelsene i den aktuelle forordningen i norsk språkdrakt. Lovavdelingen tilråder som hovedregel at forordninger gjennomføres ved inkorporasjon. Dette ivaretar hensynet til rettsenhet.

De av høringsinstansene som har uttalt seg vedrørende departementets forslag til implementeringsmåte, støtter at forordningen gjennomføres ved inkorporasjon. Departementet viser for øvrig til at instansene i all hovedsak har vært positive til forslaget, og fastholder derfor forslaget fra høringsnotatet. Siden forordning 910/2014 allerede har trådt i kraft i EU, foreslår departementet at loven trer i kraft straks. EØS-komiteen tok forordningen inn i EØS-avtalen med tilpasningstekster. I artikkel 51 skal «1. July 2017» i paragraf 3 leses som «six months after the date of entry into force of Decision of the EEA Joint Committee», og i paragraf 4 skal «from 2. July 2017» leses som «after six months from the date of entry into force of Decision of the EEA Joint Committee».

Til forordningen er det vedtatt en rekke gjennomføringsrettsakter. Disse skal i utgangspunktet inntas i norsk rett som de er. Gjennomføringsrettsaktene vil bli sendt på høring på ordinær måte.

18 Økonomiske og administrative konsekvenser

18.1 Forslaget

Rettsakten vil få administrative og økonomiske konsekvenser i forbindelse med nett-tjenester som omfattes av anerkjennelsesplikten og eventuell notifisering av norske eID-løsninger. Det må tilrettelegges for innlogging med utenlandsk eID og for at notifiserte norske eID-er kan benyttes i nett-tjenester i utlandet/EØS. Offentlige myndigheter som krever bruk av elektroniske signaturer eller segl vil iht. forordningen (art. 27 og 37) måtte anerkjenne tilsvarende signaturer eller segl fra utlandet i nærmere bestemte formater. Enklere gjenbruk av eID-er forventes imidlertid å føre til økt anvendelse av digitale selvbetjeningsløsninger både nasjonalt og på tvers i EU/EØS og følgelig medføre kostnadsbesparelser og samfunnsøkonomiske gevinster.

Et mer omfattende tilsynsregime og en rapporteringsplikt for tilsynsmyndigheten til Kommisjonen og ENISA (European Union Agency for Network and Information Security), vil videre få økonomiske og administrative konsekvenser for Nasjonal kommunikasjonsmyndighet (Nkom) som er foreslått som tilsynsmyndighet. Økte kostnader hos Nkom vil medføre økte avgifter for markedsaktørene, jf. prinsippet om at aktørene skal dekke kostnadene ved tilsynet.

Norsk akkreditering er nasjonalt akkrediteringsorgan. Et samsvarsvurderingsorgan som vil bli akkreditert i Norge, må søke om dette til Norsk akkreditering, som vurderer om organet oppfyller de krav som følger av EØS-vareloven, bestemmelsene som foreslås i det foreliggende lovforslaget, og eventuelt nærmere forskrifter.

Akkrediteringsvirksomheten finansieres gjennom gebyrer, jf. forskrift 1. juli 2013 nr. 821 om gebyrer for Norsk akkrediterings tjenester, som skal dekke samtlige kostnader for akkrediteringen.

18.2 Høringsinstansenes syn

Enkelte høringsinstanser uttrykker bekymring for at de økonomiske og administrative konsekvensene ikke er tilstrekkelig utredet. Blant annet uttaler *Finansdepartementet* at konsekvensene for Skatteetaten fremstår som uklare når det gjelder både deres arbeid med Folkeregisteret og arbeidet med skatter og avgifter. *Skattedirektoratet* påpeker at gjennomføringen av forordningen ikke må føre til lavere sikkerhet for skattlegging eller tildeling av rettigheter, og at kvaliteten i Folkeregisteret må sikres. *POD* mener at spesielt konsekvenser for norske tjenesteeiere er for dårlig belyst i høringsnotatet, og de savner også vurderinger knyttet til risiko for alle berørte parter, samt beskrivelse av mulige tiltak mot og oppfølging av svindel og misbruk.

18.3 Departementets vurdering

Innlemmelsen av forordningen innebærer i seg selv ingen vesentlige behov for tilrettelegging av norske tjenester. Det er intet krav i henhold til eIDAS-forordningen å etablere en knytning mellom den innloggede og et norsk identitetsnummer; eIDAS regulerer kun anerkjennelsen av autentiseringen. Dersom personen ikke anses tilstrekkelig identifisert for norske tjenester, vil personen ikke få tilgang.

Det vil imidlertid ofte være nødvendig at personer som logger inn med en utenlandsk eID, også kan gjenkjennes ved bruk av den norske tjenesten, hvilket i de aller fleste tilfeller vil være norsk fødselsnummer eller d-nummer. For å fullt ut oppnå gevinstene ved eID-bestemmelsene i eIDAS-forordningen og regjeringens ambisjon om grenseoverskridende tjenester bør innloggingen kunne knyttes til et norsk fødsels- eller d-nummer. Dette krever endringer i grensesnitt hos Folkeregisteret og i ID-porten. Den forventede samlede investeringskostnaden er beregnet til 16 millioner kroner og 8 millioner kroner i årlig forvaltningskostnad, fordelt mellom Skattedirektoratet og Difi.

Denne tilretteleggingen er imidlertid ikke en direkte forpliktelse etter forordningen, og er således ikke en direkte økonomisk/administrativ konsekvens av eIDAS. For tjenester hvor eIDAS gir

tilfredsstillende identifisering av personen uten slik knytning til norsk identifikator, vil eIDAS også innebære gevinster selv uten slik tilrettelegging.

Det fremgår av forordningen at erstatningsansvaret iht. artikkel 11 skal praktiseres i tråd med nasjonal rett. Departementet foreslår at det i lovens § 1 tas inn en forskriftshjemmel som gjør det mulig å sette minstekrav til erstatningsansvaret for eID-er som skal brukes i offentlig sektor.

Ved norsk notifisering av eID-løsninger vil innehavere av aktuelle eID-er få enklere tilgang til utenlandske offentlige tjenester på nett. Det må vurderes nærmere i hvilken utstrekning en unik identifikator som fødselsnummeret eller d-nummer kan følge med ved bruk av eID for tilgang til utenlandske offentlige nettjenester.

Departementet vil understreke at eIDAS ikke gir nye persongrupper rettigheter til tjenester i det norske samfunnet. Forvaltningen vil fortsatt selv fastsette sikkerhetskrav for sine løsninger, både når det gjelder krav til autentiseringsnivå og krav til identifiseringen, herunder også hvilken identitetskontroll personen har vært gjenstand for i forbindelse med registrering i Folkeregisteret. Ved at det legges til rette for anerkjennelse av eID-er på tvers av landegrensene, vil det også være større muligheter for å stille krav til elektronisk identifisering.

Etter departementets vurdering vil det påløpe noe kostnader hos Difi i forbindelse med utvikling og drift av løsninger for å håndtere notifiserte eID-løsninger gjennom ID-porten. Finansieringen vil følge prinsippene for finansiering av nasjonale felleskomponenter i tråd med forutsetningene i Meld. St. 27 (2015–2016) Digital agenda for Norge.

Tilsyn etter forordningen vil bli avgiftsfinansiert, slik tilsyn etter esignaturloven er i dag. Økte kostnader vil dermed bli finansiert ved økte avgifter. Omfanget av tilsynsoppgavene vil være avhengig av antall markedsaktører og antall tillitstjenester de tilbyr.

Innlemmelse av forordningen kan få økonomiske og administrative konsekvenser ved at Nasjonal sikkerhetsmyndighet ved SERTIT utpekes som sertifiseringsorgan. Dersom pågangen for å få sertifisert signaturfremstillingssystemer hos SERTIT øker, kan det bli behov for å styrke SERTIT med personell og kompetanseoppbygging.

Nkom anslår at de økte tilsynsoppgavene vil medføre ytterligere 1 årsverk i tillegg til eksisterende 2,5 årsverk som dekker dagens tilsynsoppgaver på området. Dersom tilsynsoppgavene viser seg å bli mer omfattende enn forutsatt, eller det blir en økning i antall nye tillitstjenester, vil antall årsverk måtte oppjusteres. Dette kan igjen få økonomiske konsekvenser for tillitstjenesteleverandørene. De sistnevnte vil også påføres økte administrative kostnader som følge av de strengere kravene til virksomhetene og kravet om hyppigere revisjoner. I siste instans vil sluttbrukerne måtte betale mer for sertifikattjenestene. Samlet sett er det departementets vurdering at endringene forordningen medfører legger til rette for tryggere handel og samhandling på nett, og at den således vil være positiv for både offentlig sektor, næringsliv og forbrukere.

Da eIDAS er en forordning, skal den lovteknisk gjennomføres som den er. Det innebærer at forordningens rettigheter og plikter blir gjeldende i Norge uavhengig av økonomiske og administrative konsekvenser som beskrevet her.

19 Merknader til de enkelte paragrafer

Til § 1

Med denne bestemmelsen gjøres forordningens regler – med de tilpasninger som følger av EØS-avtalen – til norsk lov.

Andre ledd er en forskriftshjemmel som gir Kongen adgang til å fastsette forskrifter i samsvar med forordningens bestemmelser om gjennomføringsrettsakter. For alle artikler i forordningen som hjemler at Europakommisjonen kan gi en gjennomføringsrettsakt, må det finnes en tilsvarende forskriftshjemmel slik at gjennomføringsrettsakten kan bli norsk forskrift. Andre ledd hjemler også forskrift om fastsettelse av minstekrav for erstatningsansvar for eIDer som skal brukes i offentlig sektor.

Til § 2

Begrepet elektroniske tillitstjenester dekker både tjenestene som er definert i forordningen, jf. artikkel 3, og nasjonale tillitstjenester. Se omtale under pkt. 7.3.

Til § 3

Første ledd gir Kongen adgang til å fastsette hvilket organ som skal føre tilsyn med at bestemmelsene gitt i eller i medhold av loven, blir oppfylt.

Andre til *fjerde ledd* angir en nærmere beskrivelse av tilsynsoppgavene.

Femte og *sjette ledd* gir Kongen adgang til å gi forskrift om tilsynets virksomhet, samt om fastsettelse av avgift for tjenestetilbydere som er registreringspliktige etter § 1.

Til § 4

Første ledd gir tilsynsorganet hjemmel til å ilegge tvangsmulkt for å sikre at bestemmelser gitt i eller i medhold av loven overholdes. Tvangsmulkt er et middel for å fremtvinge etterlevelse av en plikt. Begrepet «bestemmelser gitt i eller i medhold av denne loven» innebærer at plikter fastsatt i lov, forskrift eller i enkeltvedtak med hjemmel i loven, kan søkes oppfylt gjennom å ilegge tvangsmulkt. Formålet med tvangsmulkt er således ikke straff for et lovbrudd som har funnet sted, men å tvinge frem etterlevelse av plikter. Tvangsmulkten slutter derfor å løpe når plikten er oppfylt. Ileggelse av tvangsmulkt er et enkeltvedtak etter forvaltningsloven. Se merknader til § 6.

Andre ledd fastsetter tidspunkt for når tvangsmulkten begynner å løpe.

Etter *tredje ledd* kan tilsynet frafalle påløpt tvangsmulkt.

Til § 5

Første ledd hjemler straffansvar for overtredelse av nærmere angitte bestemmelser når overtredelsen er forsettlig eller grovt uaktsom. Bestemmelsen suppleres av alminnelige strafferettslige prinsipper. Straffansvaret er ikke begrenset til særskilte aktører. Overtredelser av de aktuelle bestemmelsene straffes med bøter.

Til § 6

Ifølge forvaltningsloven § 28 første ledd første punktum kan enkeltvedtak påklages til det forvaltningsorganet som er nærmest overordnet det forvaltningsorganet som har truffet vedtaket. Tilsynets vedtak i medhold av denne lov kan påklages til det organet som utpekes med hjemmel i § 6.

Klageinstansen skal utpekes av Kongen. Frist for klage reguleres av forvaltningsloven §§ 29 og 30.

Til § 7

Bestemmelsen hjemler adgang til å pålegge registreringspliktige tjenestetilbydere avgifter til finansiering av tilsynets virksomhet. Nærmere regulering vedrørende avgift vil skje i forskrift med hjemmel i denne bestemmelsen.

Til § 8

Bestemmelsen gir Kongen kompetanse til å bestemme at loven helt eller delvis skal gjelde for Svalbard og Jan Mayen.

Til § 9

Det legges opp til at loven trer i kraft straks.

Til § 10

Bestemmelsen fastsetter overgangsregler for forskrifter og enkeltvedtak gitt i medhold av lov 15. juni 2001 nr. 81 om elektronisk signatur (esignaturloven). Tilsvarende skal gjelde for utpeking av tilsynsmyndighet og klageorgan, samt eventuelle idømte erstatningskrav med hjemmel i samme lov.

Nærings- og fiskeridepartementet

t i l r å r :

At Deres Majestet godkjenner og skriver under et framlagt forslag til proposisjon til Stortinget om lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester), og samtykke til EØS-komiteens beslutning nr. 22/2018 om innlemmelse av forordningen i EØS-avtalen.

Vi HARALD, Norges Konge,

s t a d f e s t e r :

Stortinget blir bedt om å gjøre vedtak til lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester), og vedtak om samtykke til EØS-komiteens beslutning nr. 22/2018 om innlemmelse av forordningen i EØS-avtalen, i samsvar med et vedlagt forslag.

A
Forslag

til lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester)

§ 1 *eID og elektroniske tillitstjenester i EØS*

EØS-avtalen vedlegg XI Elektronisk kommunikasjon, audiovisuelle tjenester og informasjonssamfunnstjenester (forordning (EU) nr. 910/2014) om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked gjelder som lov med de tilpasninger som følger av vedlegg XI, protokoll 1 til avtalen og avtalen for øvrig.

Kongen kan gi forskrift om myndighetssamarbeid, etablering av et felles tillitsmerke, fastsettelse av sikkerhetsnivåer, etablering av rammeverk for sikring av notifiserte nasjonale eID-løsningers interoperabilitet, tillitslister, om akkreditering av samsvarsvurderingsorganer, utforming av samsvarsrevisjonsrapport og regler for gjennomføring av samsvarsrevisjoner, om krav til og sertifisering av kvalifiserte elektroniske signatur- og seglfremstillingssystemer, om kvalifiserte valideringstjenester for elektronisk signatur og elektronisk segl, om referanseformater m.m. for avansert elektronisk signatur og avansert elektronisk segl i offentlig sektor og om fastsettelse av minstekrav til erstatningsansvaret for eID-er som skal brukes i offentlig sektor.

Kongen fastsetter hvilket organ som skal være meldingsmyndighet overfor Europakommisjonen.

Kongen fastsetter hvilket organ som skal opprette, ajourføre og offentliggjøre en tillitsliste.

Kongen fastsetter hvilket organ som skal godkjenne kvalifiserte elektroniske signaturfremstillingssystemer.

§ 2 *Etablering av frivillige sertifiseringsordninger, godkjenningsordninger eller selvdeklarasjonsordninger*

I de tilfellene der det ikke allerede er et krav om det etter § 1, kan departementet for å høyne nivået for og øke tilliten til bruk av elektroniske informasjonssikkerhetstjenester gi forskrift om frivillige sertifiserings-, godkjennings- eller selvdeklarasjonsordninger, herunder hvilke krav som stilles for slike frivillige ordninger.

Departementet fastsetter hvilket organ som skal godkjenne og føre tilsyn med de frivillige ordningene.

§ 3 *Tilsyn*

Kongen fastsetter hvilket organ som skal føre tilsyn med at bestemmelsene gitt i eller i medhold av loven, blir oppfylt.

Som ledd i tilsynsvirksomheten kan tilsynsorganet gjennomføre kontroll hos virksomhetene, kreve de opplysninger og dokumenter som er nødvendige for å utføre tilsynet, og fastsette en tidsfrist for å sende dem inn.

Den som blir kontrollert, plikter å gi tilsynsorganet uhindret adgang til virksomheten, lokaler, utstyr og dokumentasjon og til å gi opplysninger og ellers medvirke til gjennomføringen av kontrollen.

Tilsynsorganet kan gi påbud om at forhold som er i strid med bestemmelser gitt i eller i medhold av denne loven, skal opphøre, og kan stille vilkår som må oppfylles for at virksomheten skal være i samsvar med loven.

Kongen kan gi forskrift om tilsynets virksomhet.

Kongen kan i forskrift bestemme at tjenestetilbydere som er registreringspliktige etter § 1, skal betale avgift. Avgiftene må ikke overstige kostnadene ved tilsynets virksomhet.

§ 4 *Tvangsmulkt*

For å sikre at bestemmelser gitt i eller i medhold av denne loven overholdes kan tilsynsorganet bestemme at en kvalifisert tjenestetilbyder skal betale en daglig løpende mulkt til staten inntil lovstridig virksomhet er opphørt eller pålegg og vilkår gitt med hjemmel i loven er etterkommet. Adgangen til å ilegge tvangsmulkt gjelder tilsva-

rende for tilsynsmyndigheten for frivillige ordninger regulert i forskrift gitt med hjemmel i § 2.

Mulkten løper ikke før klagefristen er ute. Påklages vedtaket om tvangsmulkt, løper ingen tvangsmulkt før klagesaken er avgjort, med mindre klageorganet bestemmer noe annet.

Tilsynet kan frafalle påløpt tvangsmulkt.

§ 5 *Straff*

Med bøter straffes den som forsettlig eller grovt uaktsomt

a) opptrer som utsteder av kvalifisert tillitstjeneste uten å være registrert som dette etter loven
b) unnlater å gi opplysninger etter § 3,
c) gir uriktige eller villedende opplysninger til tilsynet.

§ 6 *Klageadgang*

Tilsynets avgjørelser etter bestemmelser gitt i eller i medhold av denne loven, kan påklages til det organ Kongen utpeker.

§ 7 *Avgift*

Kongen kan gi forskrift om at tjenestetilbydere som er registreringspliktig etter loven eller etter forskrift gitt med hjemmel i § 2, skal betale avgift. Avgiften må ikke overstige kostnadene ved tilsynets virksomhet.

§ 8 *Anvendelse på Svalbard og Jan Mayen*

Kongen kan gi forskrift om lovens anvendelse på Svalbard og Jan Mayen og fastsette særlige regler under hensyn til de stedlige forhold.

§ 9 *Ikrafttredelse*

Loven gjelder fra den tid Kongen bestemmer. Fra samme tidspunkt oppheves lov 15. juni 2001 nr. 81 om elektronisk signatur.

§ 10 *Overgangsregler*

Forskrifter og enkeltvedtak gitt i medhold av lov 15. juni 2001 nr. 81 om elektronisk signatur, gjelder inntil de blir opphevet. Det samme gjelder utpeking av tilsynsmyndighet og klageorgan samt eventuelle idømte erstatningskrav med hjemmel i samme lov.

B
Forslag

til vedtak om samtykke til EØS-komiteens beslutning nr. 22/2018 om innlemmelse av forordning i EØS-avtalen

Stortinget samtykker til godkjennelse av EØS-komiteens beslutning nr. 22 av 9. februar 2018 om innlemmelse i EØS-avtalen av forordning (EU) 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner på det indre marked i samsvar med vedlagte forslag.

Vedlegg 1

EØS-komiteens beslutning nr. 22/2018 av 9. februar 2018 om endring av EØS-avtalens vedlegg XI (Elektronisk kommunikasjon, audiovisuelle tjenester og informasjonssamfunnstjenester)

EØS-KOMITEEN HAR –

under henvisning til avtalen om Det europeiske økonomiske samarbeidsområde, heretter kalt EØS-avtalen, særlig artikkel 98, og ut fra følgende betraktninger:

1) Europaparlaments- og rådsforordning (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked og om oppheving av direktiv 1999/93/EF[1] skal innlemmes i EØS-avtalen.
2) Forordning (EU) nr. 910/2014 opphever europaparlaments- og rådsdirektiv 1999/93/EF[2], som er innlemmet i EØS-avtalen, og som følgelig skal oppheves i EØS-avtalen.
3) EØS-avtalens vedlegg XI bør derfor endres –

TRUFFET DENNE BESLUTNING:

Artikkel 1

I EØS-avtalens vedlegg XI skal teksten i nr. 5l (europaparlaments- og rådsdirektiv 1999/93/EF) lyde:

«**32014 R 0910:** Europaparlaments- og rådsforordning (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked og om oppheving av direktiv 1999/93/EF (EUT L 257 av 28.8.2014, s. 73).

Forordningens bestemmelser skal for denne avtales formål gjelde med følgende tilpasning:

a) I artikkel 14 nr. 1 skal ordene ', eller mellom en EFTA-stat og den berørte tredjestat eller en internasjonal organisasjon' tilføyes etter ordene 'artikkel 218 i TEUV'.
b) Avtalepartene skal holde hverandre underrettet med hensyn til forhandlinger og inngåtte avtaler nevnt i artikkel 14 nr. 1 og, dersom det anmodes om det, holde samråd med EØS-komiteen.
c) Når Den europeiske union forhandler en avtale nevnt i artikkel 14 nr. 1, skal den søke å oppnå samme behandling for kvalifiserte tillitstjenester som leveres av kvalifiserte tilbydere av tillitstjenester etablert i EFTA-statene.
d) I artikkel 51, når det gjelder EFTA-statene:
   i) i nr. 3 skal ordene '1. juli 2017' forstås som 'seks måneder etter den dag EØS-komiteens beslutning nr. 22/2018 av 9. februar 2018 trer i kraft',
   ii) i nr. 4 skal ordene 'fra 2. juli 2017' forstås som 'seks måneder etter den dag EØS-komiteens beslutning nr. 22/2018 av 9. februar 2018 trer ikraft'.»

Artikkel 2

Teksten til forordning (EU) nr. 910/2014 på islandsk og norsk, som skal kunngjøres i EØS-tillegget til *Den europeiske unions tidende*, skal gis gyldighet.

Artikkel 3

Denne beslutning trer i kraft 10. februar 2018, forutsatt at alle meddelelser etter EØS-avtalens artikkel 103 nr. 1 er inngitt (*).

Artikkel 4

Denne beslutning skal kunngjøres i EØS-avdelingen av og EØS-tillegget til *Den europeiske unions tidende.*

Utferdiget i Brussel 9. februar 2018.
For EØS-komiteen
Claude Maerten
Formann

[1] EUT L 257 av 28.8.2014, s. 73.
[2] EFT L 13 av 19.1.2000, s. 12.

* Forfatningsrettslige krav angitt