STORTINGET

Innst. 332 S

(2017–2018)

Innstilling til Stortinget
fra næringskomiteen

Prop. 71 LS (2017–2018)

Innstilling fra næringskomiteen om samtykke til godkjennelse av EØS-komiteens beslutning nr. 22/2018 om innlemmelse i EØS-avtalen av forordning (EU) 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner på det indre marked

Til Stortinget

1. Sammendrag

1.1 Proposisjonens hovedinnhold

Nærings- og fiskeridepartementet foreslår i 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. Forordningen skal 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 fremmes som følge av at EØS-komiteen ved beslutning nr. 22 av 9. februar 2018 vedtok 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).

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

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 regulering 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.

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.

Begreper i proposisjonen

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.

Kravspesifikasjon for PKI er en overordnet, funksjonell kravspesifikasjon for selvdeklarering og anskaffelse av PKI-løsninger, herunder PKI-baserte eID-løsninger.

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.

Elektronisk segl er mekanismer som knytter et dokument til en juridisk person som har forseglet dokumentet. Begrepet er teknologinøytralt.

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.

1.2 Bakgrunnen for lovforslaget

En effektiv og hensiktsmessig digital samhandling forutsetter at alle aktørene har tillit til at elektroniske transaksjoner skjer på en trygg måte. EU har forsøkt å møte denne utfordringen gjennom forordning 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked. 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.

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

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

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

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

Forordningen har til hensikt å sikre et velfungerende indre marked, samtidig som man ivaretar et adekvat sikkerhetsnivå for elektronisk identifikasjon (eID) og tillitstjenester. 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.

Behandling av personopplysninger skal skje i samsvar med EUs personverndirektiv (direktiv 95/46/EF). I fortalen 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.

Forordningen 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. 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.

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.

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.

1.4 Arbeidet med regelverket i EU og Norge

De gjennomføringsrettsaker som er vedtatt fram til nå, er listet opp i kapittel 4 i proposisjonen. EØS-posisjonsnotater om disse rettsaktene publiseres i EØS-notatbasen fortløpende. Forordningen inneholder også bestemmelser om gjennomføringsrettsakter og delegerte rettsakter som Kommisjonen «kan» gjennomføre.

Nærings- og fiskeridepartementet sender 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.

Høringsinstansene er langt på vei positive både til innføringen av forordningen med gjennomføringsrettsakter i norsk lov og til samtidig opphevelse av esignaturloven. De fleste instansene som har uttalt seg, anser forordningen som et viktig verktøy for å understøtte samarbeid og handel mellom aktører i EU/EØS-området. 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 er gjennomgått tematisk i proposisjonen.

1.5 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.

De av høringsinstansene som har uttalt seg vedrørende forslag til implementeringsmåte, støtter at forordningen gjennomføres ved inkorporasjon. Siden forordning 910/2014 allerede har trådt i kraft i EU, foreslår departementet at loven trer i kraft straks.

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.

1.6 Økonomiske og administrative konsekvenser

Innlemmelsen av forordningen innebærer i seg selv ingen vesentlige behov for tilrettelegging av norske tjenester. 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. 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 mill. kroner og 8 mill. kroner i årlig forvaltningskostnad, fordelt mellom Skattedirektoratet og Difi.

Denne tilretteleggingen er imidlertid ikke en direkte forpliktelse etter forordningen og er derfor 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.

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 understreker 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 identifisering.

Det vil påløpe noe kostnader hos Difi i forbindelse med utvikling og drift av løsninger for å håndtere notifiserte eID-løsninger gjennom ID-porten.

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 til-

litstjenester, 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 de økonomiske og administrative konsekvenser som er beskrevet i proposisjonen.

Når det gjelder forslag til ny lov som er nødvendig for å gjennomføre forordningen, vises det til egen innstilling, Innst. 331 L (2017–2018).

2. Komiteens merknader

Komiteen, medlemmene fra Arbeiderpartiet, Ruth Grung, Cecilie Myrseth, Nils Kristen Sandtrøen og Terje Aasland, fra Høyre, Margunn Ebbesen, Ingunn Foss, Kårstein Eidem Løvaas og Tom-Christer Nilsen, fra Fremskrittspartiet, Kjell-Børge Freiberg og Morten Ørsal Johansen, fra Senterpartiet, Geir Adelsten Iversen og lederen Geir Pollestad, fra Sosialistisk Venstreparti, Torgeir Knag Fylkesnes, fra Venstre, André N. Skjelstad, og fra Kristelig Folkeparti, Steinar Reiten, viser til at det her gis samtykke til EØS-komiteens beslutning nr. 22/2018 om innlemmelse av forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked i EØS-avtalen. Komiteen viser til at det har vært en lang prosess i EU og i Norge for å komme frem til forordningen slik den nå foreligger. Komiteen viser til at en forordning skal vedtas slik den er, i motsetning til et EU-direktiv, hvor hvert land kan gjøre sine tilpasninger i forhold til nasjonal rett.

Komiteen viser til at forordningen skal legge til rette for økt elektronisk samhandling mellom næringsdrivende, borgere og offentlige myndigheter på tvers av landegrensene i EU/EØS, og dermed gi sterkere økonomisk vekst i det indre marked. Videre viser komiteen til at forordningen utvider området for reguleringen av elektroniske tillitstjenester sammenliknet med hva esignaturdirektivet omfattet, og styrker dagens regler om elektronisk signatur. Komiteen viser til at proposisjonen omtaler at 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. Komiteen er av den oppfatning at forordningen er et viktig verktøy i digitaliseringsprosessen, og at den vil bidra til å skape trygghet og tillit på nett.

Komiteen viser til at 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.

Komiteen viser til at innlemmelse av forordningen i seg selv ikke innebærer vesentlige behov for tilrettelegging av norske tjenester. Imidlertid vil det være behov for endringer i grensesnitt hos Folkeregisteret og i ID-porten hvis en fullt ut skal oppnå gevinstene ved eID-bestemmelsene i eIDAS-forordningen. Dette hvis en har ambisjon om grenseoverskridende tjenester. Komiteen viser til at den samlede investeringskostnaden da er beregnet til 16 mill. kroner og 8 mill. kroner i årlig forvaltningskostnad, fordelt mellom Skattedirektoratet og Difi. Komiteen viser videre til at denne tilretteleggingen imidlertid ikke er 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.

Komiteen viser også til brev av 23. april 2018 med vedlegg fra statsråd Torbjørn Røe Isaksen til Stortingets presidentskap. Brevet med vedlegg er vedlagt innstillingen.

Komiteen viser for øvrig til proposisjonen og til merknader i separat innstilling om lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det videre marked (lov om elektroniske tillitstjenester).

3. Uttalelse fra utenriks- og forsvarskomiteen

Komiteens utkast til innstilling ble 15. mai 2018 oversendt til utenriks- og forsvarskomiteen for uttalelse.

Utenriks- og forsvarskomiteen uttaler følgende i brev av 24. mai 2018:

«Utenriks og forsvarskomiteens medlemmer slutter seg til næringskomiteens utkast til innstilling til Prop. 71 LS (2017–2018), og har ingen ytterligere merknader.»

4. Komiteens tilråding

Komiteens tilråding fremmes av en samlet komité.

K o m i t e e n har for øvrig ingen merknader, viser til proposisjonen og rår Stortinget til å gjøre følgende

v e d t a k :

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.

Oslo, i næringskomiteen, 28. mai 2018

Geir Pollestad
leder

Margunn Ebbesen
ordfører

Vedlegg 1

Brev fra Nærings- og fiskeridepartementet v/statsråd Torbjørn Røe Isaksen til Stortingets presidentskap, datert 23. april 2018

Rettelse av begrep i lovforslag til Prop. 71 LS (2017-2018)

Jeg viser til Prop. 71 LS (2017–2018) 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, som er til behandling i næringskomiteen.

Ved en inkurie ble ikke begrepet *informasjonssikkerhetstjenester* endret til begrepet *tillitstjenester* i lovforslaget § 2. Begrepet informasjonssikkerhetstjenester ble benyttet da lovforslaget var på åpen høring, men begrepet tillitstjenester ble senere vurdert å være mer dekkende og språklig mer forståelig. Begrepet tillitstjenester er benyttet gjennomgående i hele proposisjonsteksten, men ble altså ikke endret i selve lovforslaget. Vedlagt følger lovforslaget slik det var ment å ligge ved proposisjonen. Jeg foreslår at Stortinget legger den rettede versjonen til grunn i sin vurdering og eventuelle vedtakelse av lovforslaget.

Vedlagt følger også en norsk oversettelse av selve forordningen, som burde ha fulgt som vedlegg til Prop 71 LS.

Vedlegg 2

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

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

EUROPAPARLAMENTET OG RÅDET FOR DEN EUROPEISKE UNION HAR—

under henvisning til traktaten om Den europeiske unions virkemåte, særlig artikkel 114,

under henvisning til forslag fra Europakommisjonen,

etter oversending av utkast til regelverksakt til de nasjonale parlamentene,

under henvisning til uttalelse fra Den europeiske økonomiske og sosiale komité([1]),

etter den ordinære regelverksprosessen([2]) og

ut fra følgende betraktninger:

1) Med henblikk på den økonomiske og sosiale utvikling er det av avgjørende betydning at det skapes tillit til internettmiljøet. Manglende tillit, særlig på grunn av en følelse av manglende rettssikkerhet, gjør at forbrukere, foretak og offentlige myndigheter nøler med å gjennomføre transaksjoner elektronisk og å ta i bruk nye tjenester.
2) Formålet med denne forordning er å styrke tilliten til elektroniske transaksjoner i det indre marked ved å skape et felles grunnlag for sikker elektronisk samhandling mellom borgere, foretak og offentlige myndigheter, og på den måten øke effektiviteten i offentlige og private nettbaserte tjenester, elektronisk forretningsvirksomhet og elektronisk handel i Unionen.
3) Europaparlaments- og rådsdirektiv 1999/93/EF([3]) omhandlet elektroniske signaturer uten at det ble fastsatt en fullstendig ramme for sikre, pålitelige og brukervennlige elektroniske transaksjoner på tvers av landegrensene og på tvers av sektorer. Ved denne forordning styrkes og utvides regelverket i nevnte direktiv.
4) I kommisjonsmeldingen av 26. august 2010 med tittelen «A Digital Agenda for Europe» påpekes det at fragmenteringen av det digitale markedet, manglende samvirkingsevne og økende nettkriminalitet utgjør vesentlige hindringer for en positiv utvikling i den digitale økonomien. I sin rapport om EU-borgerskap fra 2010 med tittelen «Dismantling the obstacles to EU citizens' rights» understreket Kommisjonen også behovet for å løse de største problemene som er til hinder for at EU-borgerne kan dra nytte av fordelene ved et digitalt indre marked og digital tjenesteyting over landegrensene.
5) I sine konklusjoner av 4. februar 2011 og 23. oktober 2011 oppfordret Det europeiske råd Kommisjonen til å skape et digitalt indre marked innen 2015, til å gjøre raske framskritt på sentrale områder i den digitale økonomien og til å fremme et fullstendig integrert digitalt indre marked ved å forenkle bruken av nettbaserte tjenester over landegrensene, med særlig vekt på å fremme sikker elektronisk identifikasjon og autentisering.
6) I sine konklusjoner av 27. mai 2011 oppfordret Rådet Kommisjonen til å bidra til det digitale indre marked ved å skape egnede vilkår for gjensidig anerkjennelse over landegrensene av sentrale verktøy, for eksempel elektronisk identifikasjon, elektroniske dokumenter, elektroniske signaturer og elektroniske leveringstjenester, samt for samvirkende e-forvaltningstjenester i hele Den europeiske union.
7) I sin resolusjon av 21. september 2010 om gjennomføring av det indre marked for elektronisk handel([4]) understreket Europaparlamentet viktigheten av sikkerhet i forbindelse med elektroniske tjenester, særlig elektroniske signaturer, samt behovet for å opprette en infrastruktur for offentlige nøkler på felleseuropeisk plan, og oppfordret Kommisjonen til å opprette en portal for europeiske valideringsmyndigheter for å sikre elektroniske signaturers samvirkingsevne over landegrensene og øke sikkerheten for transaksjoner som utføres via internett.
8) I henhold til europaparlaments- og rådsdirektiv 2006/123/EF([5]) skal medlemsstatene opprette «felles kontaktpunkter» for å sikre at alle framgangsmåter og formaliteter knyttet til tilgang til en tjenestevirksomhet og utøvelsen av denne kan gjennomføres på en enkel måte, på avstand og elektronisk, via

1. EUT C 351 av 15.11.2012, s. 73.
2. Europaparlamentets holdning av 3. april 2014 (ennå ikke offentliggjort i EUT) og rådsbeslutning av 23. juli 2014.
3. Europaparlaments- og rådsdirektiv 1999/93/EF av 13. desember 1999 om en fellesskapsramme for elektroniske signaturer (EFT L 13 av 19.1.2000, s. 12).
4. EUT C 50 E av 21.2.2012, s. 1
5. Europaparlaments- og rådsdirektiv 2006/123/EF av 12. desember 2006 om tjenester i det indre marked (EUT L 376 av 27.12.2006, s. 36).

det egnede felles kontaktpunktet hos vedkommende myndigheter. En rekke nettbaserte tjenester som er tilgjengelige via felles kontaktpunkter, krever elektronisk identifikasjon, autentisering og signatur.

9) I de fleste tilfeller kan borgerne ikke bruke sin elektroniske identifikasjon til å autentisere seg i en annen medlemsstat, ettersom de nasjonale ordningene for elektronisk identifikasjon i deres stat ikke er anerkjent i andre medlemsstater. Denne elektroniske barrieren hindrer tjenestetilbydere i å få fullt utbytte av fordelene ved det indre marked. Gjensidig anerkjente elektroniske identifikasjonsmidler vil gjøre det lettere å tilby en lang rekke tjenester over landegrensene i det indre marked og gjøre det mulig for foretak å drive virksomhet over landegrensene uten å støte på en rekke hindringer i kontakten med offentlige myndigheter.

10) Ved europaparlaments- og rådsdirektiv 2011/24/EU([1]) opprettes det et nettverk av nasjonale myndigheter med ansvar for e-helse. For å øke sikkerheten og kontinuiteten i forbindelse med helsetjenester over landegrensene skal nettverket utarbeide retningslinjer for tilgang over landegrensene til elektroniske helseopplysninger og -tjenester, herunder ved å støtte felles identifikasjons- og autentiseringstiltak for å lette overføringen av opplysninger i forbindelse med helsetjenester over landegrensene. Gjensidig anerkjennelse av elektronisk identifikasjon og autentisering er en forutsetning for at helsetjenester over landegrensene skal bli virkelighet for borgerne i Unionen. Når borgerne reiser til en annen stat for å få behandling, må opplysningene om deres helse være tilgjengelige i den staten der behandlingen skal utføres. Dette krever en robust, sikker og pålitelig ramme for elektronisk identifikasjon.

11) Denne forordning bør få anvendelse i fullt samsvar med prinsippene om vern av personopplysninger fastsatt i europaparlaments- og rådsdirektiv 95/46/EF([2]). Når det gjelder prinsippet om gjensidig anerkjennelse som fastsettes ved denne forordning, bør autentisering for en nettbasert tjeneste bare omfatte behandling av identifikasjonsdata som er tilstrekkelige og relevante og ikke omfatter mer enn det som kreves for å gi tilgang til den nettbaserte tjenesten. Videre bør tilbydere av tillitstjenester og tilsynsorganer oppfylle kravene til fortrolig og sikker behandling i direktiv 95/46/EF.

12) Ett av målene med denne forordning er å fjerne eksisterende hindringer for medlemsstatenes bruk over landegrensene av elektroniske identifikasjonsmidler ved autentisering, i det minste for offentlige tjenester. Denne forordning har ikke som mål å gripe inn i systemer for forvaltning av elektroniske identiteter og tilhørende infrastruktur som er opprettet i medlemsstatene. Målet med denne forordning er å sikre at sikker identifikasjon og autentisering er mulig når det gjelder tilgang til nettbaserte tjenester som tilbys av medlemsstatene over landegrensene.

13) Medlemsstatene bør stå fritt til å benytte eller innføre elektroniske identifikasjonsmidler i forbindelse med tilgang til nettbaserte tjenester. De bør i tillegg selv kunne bestemme om privat sektor også skal kunne tilby disse midlene. Medlemsstatene bør ikke være forpliktet til å melde sine ordninger for elektronisk identifikasjon til Kommisjonen. Medlemsstatene kan velge å melde til Kommisjonen alle, noen eller ingen av ordningene for elektronisk identifikasjon som brukes på nasjonalt plan for å få tilgang til i det minste offentlige nettbaserte tjenester eller spesifikke tjenester.

14) I denne forordning må det fastsettes visse vilkår med hensyn til hvilke elektroniske identifikasjonsmidler som må anerkjennes, og hvordan ordningene for elektronisk identifikasjon bør meldes. Vilkårene bør bidra til at medlemsstatene kan bygge opp den nødvendige tillit til hverandres ordninger for elektronisk identifikasjon, og til gjensidig anerkjennelse av elektroniske identifikasjonsmidler som faller inn under deres meldte ordninger. Prinsippet om gjensidig anerkjennelse bør få anvendelse dersom meldermedlemsstatens ordning for elektronisk identifikasjon oppfyller vilkårene for melding og meldingen er offentliggjort i *Den europeiske unions tidende*. Prinsippet om gjensidig anerkjennelse bør imidlertid bare gjelde autentisering for en nettbasert tjeneste. Tilgangen til slike nettbaserte tjenester og den endelige leveringen av disse til den som etterspør tjenestene, bør være nært knyttet til retten til å motta slike tjenester på vilkårene fastsatt i nasjonal lovgivning.

15) Plikten til å anerkjenne elektroniske identifikasjonsmidler bør bare gjelde midler som har et identitetssikkerhetsnivå som tilsvarer eller er høyere enn nivået som kreves for den aktuelle nettbaserte tjenesten. Plikten bør dessuten gjelde bare når det aktuelle offentlige organet benytter sikkerhetsnivået «betydelig» eller «høyt» i forbindelse med tilgang til den nettbaserte tjenesten. Medlemsstatene bør i samsvar med unionsretten stå fritt til å aner-

1. Europaparlaments- og rådsdirektiv 2011/24/EU av 9. mars 2011 om anvendelse av pasientrettigheter ved helsetjenester over landegrensene (EUT L 88 av 4.4.2011, s. 45).
2. Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (EFT L 281 av 23.11.1995, s. 31)

kjenne elektroniske identifikasjonsmidler med lavere identitetssikkerhetsnivå.

16) Sikkerhetsnivåene bør gjenspeile graden av tillit til et elektronisk identifikasjonsmiddel når det gjelder å fastslå identiteten til en person, og dermed være en garanti for at personen som gjør krav på en bestemt identitet, faktisk er den som har fått tildelt identiteten. Sikkerhetsnivået avhenger av graden av tillit som elektroniske identifikasjonsmidler gir når det gjelder en persons påståtte identitet, idet det tas hensyn til prosesser (for eksempel bekreftelse og kontroll av identitet samt autentisering), forvaltningsvirksomhet (for eksempel enheten som utsteder elektroniske identifikasjonsmidler og framgangsmåten for å utstede slike midler) og tekniske kontroller som er gjennomført. Det finnes en rekke tekniske definisjoner og beskrivelser av sikkerhetsnivåer som følge av EU-finansierte omfattende forsøksprosjekter, standardiseringer og internasjonale aktiviteter. I det omfattende forsøksprosjektet STORK samt i ISO 29115 vises det blant annet til nivå 2, 3 og 4 som det bør tas nøye hensyn til ved fastsettelse av tekniske minstekrav, minstestandarder og minstekrav til framgangsmåter for sikkerhetsnivåene «lavt», «betydelig» og «høyt» i henhold til denne forordning, samtidig som det sikres en ensartet anvendelse av denne forordning, særlig med hensyn til sikkerhetsnivået «høyt» i forbindelse med kontroll av identitet ved utstedelse av kvalifiserte sertifikater. De fastsatte kravene bør være teknologinøytrale. Det bør være mulig å oppfylle de nødvendige sikkerhetskravene ved hjelp av forskjellig teknologi.

17) Medlemsstatene bør oppmuntre privat sektor til frivillig å benytte elektroniske identifikasjonsmidler som faller inn under en meldt ordning, til identifikasjonsformål når dette er nødvendig for nettbaserte tjenester eller elektroniske transaksjoner. Muligheten til å benytte slike elektroniske identifikasjonsmidler vil gjøre det mulig for privat sektor å benytte elektronisk identifikasjon og autentisering som allerede i stor utstrekning benyttes i mange medlemsstater, i det minste i forbindelse med offentlige tjenester, og gjøre det enklere for foretak og borgere å få tilgang til deres nettbaserte tjenester over landegrensene. For å gjøre det enklere for privat sektor å benytte slike elektroniske identifikasjonsmidler over landegrensene bør autentiseringsmuligheten som tilbys av en medlemsstat, være tilgjengelig for tjenestebrukere i privat sektor som er etablert utenfor medlemsstatens territorium, på samme vilkår som dem som gjelder for tjenestebrukere i privat sektor som er etablert i medlemsstaten. Når det gjelder tjenestebrukere i privat sektor, kan meldermedlemsstaten derfor definere vilkår for tilgang til autentiseringsmidlene. Slike vilkår for tilgang kan inneholde opplysninger om hvorvidt autentiseringsmidlene knyttet til den meldte ordningen er tilgjengelig for tjenestebrukere i privat sektor.

18) Ved denne forordning bør det fastsettes hvilket erstatningsansvar meldermedlemsstaten, parten som utsteder det elektroniske identifikasjonsmiddelet, og parten som utfører framgangsmåten for autentisering, skal ha dersom de relevante forpliktelsene i henhold til denne forordning ikke oppfylles. Denne forordning bør imidlertid få anvendelse i samsvar med nasjonale regler for erstatningsansvar. Den berører derfor ikke nasjonale regler for f.eks. definisjon av skader eller gjeldende relevante saksbehandlingsregler, herunder bevisregler.

19) Sikkerheten i ordninger for elektronisk identifikasjon er av avgjørende betydning med tanke på pålitelig gjensidig anerkjennelse over landegrensene av elektroniske identifikasjonsmidler. I denne forbindelse bør medlemsstatene samarbeide om sikkerheten og samvirkingsevnen til ordningene for elektronisk identifikasjon på EU-plan. Dersom det i ordningene for elektronisk identifikasjon kreves at tjenestebrukere skal benytte spesifikk maskinvare eller programvare på nasjonalt plan, innebærer samvirkingsevne over landegrensene at medlemsstatene ikke pålegger tjenestebrukere som er etablert utenfor medlemsstatens territorium, slike krav og tilhørende kostnader. I dette tilfellet bør egnede løsninger drøftes og utvikles innenfor rammen av samvirkingsevne. Tekniske krav som skyldes de iboende spesifikasjonene for nasjonale elektroniske identifikasjonsmidler, og som kan påvirke innehaverne av slike elektroniske midler (for eksempel smartkort), er imidlertid uunngåelig.

20) Medlemsstatenes samarbeid bør fremme den tekniske samvirkingsevnen til de meldte ordningene for elektronisk identifikasjon med henblikk på å oppnå en høy grad av tillit og sikkerhet som er tilpasset graden av risiko. Utveksling av opplysninger og beste praksis mellom medlemsstatene med henblikk på gjensidig anerkjennelse bør bidra til dette samarbeidet.

21) Ved denne forordning bør det også fastsettes en generell rettslig ramme for bruk av tillitstjenester. Det bør imidlertid ikke innføres en generell plikt til å benytte dem eller til å opprette et tilgangspunkt for alle eksisterende tillitstjenester. Denne forordning bør særlig ikke omfatte levering av tjenester som utelukkende benyttes i lukkede systemer mellom en definert gruppe av deltakere, og som ikke påvirker tredjeparter. Systemer som er opprettet i foretak eller innen offentlig forvaltning for å håndtere interne prosesser, og der det benyttes tillitstje-

nester, bør for eksempel ikke omfattes av kravene i denne forordning. Det er bare tillitstjenester som tilbys offentligheten, og som påvirker tredjeparter, som bør oppfylle kravene fastsatt i denne forordning. Denne forordning bør heller ikke omfatte aspekter knyttet til inngåelse og gyldighet av kontrakter eller andre juridiske forpliktelser dersom det i nasjonal lovgivning eller unionsretten er fastsatt formkrav. Den bør heller ikke berøre nasjonale formkrav som gjelder for offentlige registre, særlig handelsregistre eller matrikler.

22) For å bidra til utstrakt bruk over landegrensene av tillitstjenester bør det i alle medlemsstater være mulig å benytte tjenestene som bevis i forbindelse med rettergang. Rettsvirkningene av tillitstjenester skal defineres i nasjonal lovgivning, med mindre annet er fastsatt i denne forordning.

23) I den grad det ved denne forordning innføres en plikt til å anerkjenne en tillitstjeneste, kan en slik tjeneste avvises bare dersom den som plikten er rettet mot, av tekniske årsaker som ligger utenfor vedkommendes umiddelbare kontroll, ikke er i stand til å lese eller kontrollere den. Plikten bør imidlertid ikke i seg selv medføre at et offentlig organ må anskaffe den maskinvaren og programvaren som er nødvendig for å sikre at alle eksisterende tillitstjenester er teknisk lesbare.

24) Medlemsstatene kan i samsvar med unionsretten opprettholde eller innføre nasjonale bestemmelser om tillitstjenester, så lenge tjenestene ikke harmoniseres fullt ut ved denne forordning. Tillitstjenester som oppfyller kravene i denne forordning, bør imidlertid omfattes av fri bevegelighet i det indre marked.

25) Medlemsstatene bør stå fritt til å definere andre typer tillitstjenester i tillegg til dem som er oppført på den lukkede listen over tillitstjenester fastsatt i denne forordning, og anerkjenne dem på nasjonalt plan som kvalifiserte tillitstjenester.

26) På grunn av den raske teknologiske utviklingen bør det ved denne forordning vedtas en strategi som er åpen for nyskaping.

27) Denne forordning bør være teknologinøytral. De rettsvirkninger den medfører, bør kunne oppnås ved hjelp av et hvilket som helst teknisk middel, forutsatt at kravene i denne forordning er oppfylt.

28) For å styrke særlig små og mellomstore bedrifters og forbrukernes tillit til det indre marked og fremme bruken av tillitstjenester og -produkter bør begrepene kvalifiserte tillitstjenester og kvalifisert tilbyder av tillitstjenester innføres for å definere krav og forpliktelser som sikrer et høyt nivå av sikkerhet for alle kvalifiserte tillitstjenester og -produkter som benyttes eller tilbys.

29) I tråd med forpliktelsene i FNs konvensjon om rettighetene til personer med nedsatt funksjonsevne, godkjent ved rådsbeslutning 2010/48/EF([1]), særlig artikkel 9 i konvensjonen, bør personer med nedsatt funksjonsevne ha mulighet til å benytte tillitstjenester og sluttbrukerprodukter som benyttes ved levering av tjenestene, på lik linje med andre forbrukere. Når det er mulig, bør tillitstjenester og sluttbrukerprodukter som benyttes ved levering av tjenestene, derfor være tilgjengelige for personer med nedsatt funksjonsevne. Vurderingen av gjennomførbarhet bør blant annet omfatte tekniske og økonomiske hensyn.

30) Medlemsstatene bør utpeke ett eller flere tilsynsorganer med ansvar for å utføre tilsynsvirksomheten i henhold til denne forordning. Medlemsstatene bør også, etter en gjensidig avtale med en annen medlemsstat, kunne beslutte å utpeke et tilsynsorgan på den andre medlemsstatens territorium.

31) Tilsynsorganene bør samarbeide med personvernmyndighetene, for eksempel ved å underrette dem om resultatene av revisjoner av kvalifiserte tilbydere av tillitstjenester, ved mistanke om brudd på reglene for vern av personopplysninger. Opplysningene bør særlig omfatte sikkerhetshendelser og brudd på personopplysningssikkerheten.

32) For å øke brukernes tillit til det indre marked bør det påligge alle tilbydere av tillitstjenester å følge en god sikkerhetspraksis som er tilpasset risikoene knyttet til deres virksomhet.

33) Bestemmelser om bruk av pseudonymer i sertifikater bør ikke hindre medlemsstatene i å kreve identifikasjon av personer i henhold til unionsretten eller nasjonal lovgivning.

34) Alle medlemsstater bør følge felles grunnleggende tilsynskrav for å sikre et sammenlignbart sikkerhetsnivå for kvalifiserte tillitstjenester. For å fremme en ensartet anvendelse av disse kravene i hele Unionen bør medlemsstatene vedta sammenlignbare framgangsmåter og utveksle opplysninger om sin tilsynsvirksomhet og beste praksis på området.

35) Alle tilbydere av tillitstjenester bør omfattes av kravene i denne forordning, særlig dem som gjelder sikkerhet og erstatningsansvar, for å sikre nødvendig aktsomhet, innsyn og ansvarlighet i deres virksomhet og tjenester. Med hensyn til den type tjenester som tilbydere av tillitstjenester leverer, bør det med tanke på nevnte krav imidlertid skilles mellom kvalifiserte og ikke-kvalifiserte tilbydere av tillitstjenester.

---

1. Rådsbeslutning 2010/48/EF av 26. november 2009 om Det europeiske fellesskaps inngåelse av De forente nasjoners konvensjon om rettighetene til personer med nedsatt funksjonsevne (EUT L 23 av 27.1.2010, s. 35)

36) Innføring av en tilsynsordning for alle tilbydere av tillitstjenester bør sikre like vilkår når det gjelder sikkerhet og ansvarlighet i forbindelse med deres virksomhet og tjenester, og dermed bidra til vern av brukere og til det indre markeds virkemåte. Ikke-kvalifiserte tilbydere av tillitstjenester bør omfattes av et mindre omfattende og reaktivt tilsyn i ettertid som er tilpasset deres type tjenester og virksomhet. Tilsynsorganet bør derfor ikke ha en generell plikt til å føre tilsyn med ikke-kvalifiserte tjenestetilbydere. Tilsynsorganet bør treffe tiltak bare når det underrettes (for eksempel av den ikke-kvalifiserte tilbyderen av tillitstjenester selv, av et annet tilsynsorgan, ved en melding fra en bruker eller en forretningspartner eller på grunnlag av egne undersøkelser) om at en ikke-kvalifisert tilbyder av tillitstjenester ikke oppfyller kravene i denne forordning.

37) Denne forordning bør fastsette erstatningsansvaret til alle tilbydere av tillitstjenester. Ved denne forordning innføres det særlig en ansvarsordning som innebærer at alle tilbydere av tillitstjenester bør være ansvarlige for skader påført fysiske eller juridiske personer på grunn av manglende overholdelse av forpliktelsene i denne forordning. For å forenkle vurderingen av de finansielle risikoene som tilbydere av tillitstjenester eventuelt vil måtte bære, eller som de bør forsikre seg mot, tillates det ved denne forordning at tilbydere av tillitstjenester på visse vilkår kan fastsette begrensninger for bruken av tjenestene de leverer, og frasi seg ansvaret for skader oppstått som følge av bruk av tjenester som overskrider disse begrensningene. Kundene bør på behørig vis opplyses om begrensningene på forhånd. Begrensningene bør være mulig å gjenkjenne for en tredjepart, for eksempel ved at opplysninger om begrensningene angis i vilkårene for tjenesten som leveres, eller ved hjelp av andre gjenkjennelige midler. For at disse prinsippene skal kunne gjennomføres, bør denne forordning få anvendelse i samsvar med nasjonale regler for erstatningsansvar. Denne forordning berører derfor ikke nasjonale regler for f.eks. definisjon av skader, forsett og uaktsomhet eller gjeldende relevante saksbehandlingsregler.

38) Det er svært viktig at sikkerhetsbrudd samt sikkerhetsrisikovurderinger meldes, slik at berørte parter kan få hensiktsmessige opplysninger ved sikkerhetsbrudd eller tap av integritet.

39) For å gjøre det mulig for Kommisjonen og medlemsstatene å vurdere effektiviteten av ordningen for melding av brudd som innføres ved denne forordning, bør det kreves at tilsynsorganer framlegger sammenfattende opplysninger for Kommisjonen og Den europeiske unions byrå for nett- og informasjonssikkerhet (ENISA).

40) For å gjøre det mulig for Kommisjonen og medlemsstatene å vurdere effektiviteten av den utvidede tilsynsordningen som innføres ved denne forordning, bør det kreves at tilsynsorganer rapporterer om sin virksomhet. Dette vil bidra til å fremme utvekslingen av god praksis mellom tilsynsorganene og gjøre det mulig å kontrollere at alle vesentlige tilsynskrav gjennomføres på en ensartet og effektiv måte i alle medlemsstater.

41) For å sikre at kvalifiserte tillitstjenester er bærekraftige og varige og for å øke brukernes tillit til kontinuiteten i kvalifiserte tillitstjenester, bør tilsynsorganer kontrollere om det foreligger bestemmelser om planer for opphør av virksomhet, og om de anvendes på riktig måte, i de tilfeller der kvalifiserte tilbydere av tillitstjenester innstiller sin virksomhet.

42) For å forenkle tilsynet med kvalifiserte tilbydere av tillitstjenester, for eksempel dersom en tjenestetilbyder leverer sine tjenester på en annen medlemsstats territorium og ikke omfattes av tilsyn der, eller dersom en tjenestetilbyders datamaskiner er plassert på territoriet til en annen medlemsstat enn der tjenestetilbyderen er etablert, bør det opprettes et system for gjensidig bistand mellom tilsynsorganene i medlemsstatene.

43) For å sikre at kvalifiserte tilbydere av tillitstjenester og tjenestene de leverer, oppfyller kravene fastsatt i denne forordning, bør et samsvarsvurderingsorgan foreta en samsvarsvurdering, og de kvalifiserte tilbyderne av tillitstjenester bør framlegge samsvarsvurderingsrapportene for tilsynsorganet. Når tilsynsorganet krever at en kvalifisert tilbyder av tillitstjenester skal framlegge en ad hoc-samsvarsvurderingsrapport, bør tilsynsorganet særlig overholde prinsippene om god forvaltning, herunder plikten til å begrunne sine beslutninger, samt forholdsmessighetsprinsippet. Tilsynsorganet bør derfor behørig begrunne sin beslutning om å kreve en ad hoc-samsvarsvurdering.

44) Formålet med denne forordning er å fastsette en konsekvent ramme som sikrer et høyt sikkerhets- og rettssikkerhetsnivå for tillitstjenester. I denne forbindelse bør Kommisjonen ved behandling av samsvarsvurderingen av produkter og tjenester, når det er hensiktsmessig, søke å oppnå synergier med eksisterende relevante europeiske og internasjonale ordninger, for eksempel europaparlaments- og rådsforordning (EF) nr. 765/2008([1]) der det fastsettes krav til akkreditering av samsvarsvurderingsorganer og markedstilsyn for produkter.

1. Europaparlaments- og rådsforordning (EF) nr. 765/2008 av 9. juli 2008 om fastsettelse av kravene til akkreditering og markedstilsyn for markedsføring av produkter, og om oppheving av forordning (EØF) nr. 339/93 (EUT L 218 av 13.8.2008, s. 30).

45) For å muliggjøre en effektiv iverksettelsesprosess som bør føre til at kvalifiserte tilbydere av tillitstjenester og de kvalifiserte tillitstjenestene de leverer, oppføres på tillitslister, bør det oppmuntres til innledende kontakt mellom potensielle kvalifiserte tilbydere av tillitstjenester og vedkommende tilsynsorgan for å legge til rette for kontrollen i forkant av levering av kvalifiserte tillitstjenester.

46) Tillitslister er av avgjørende betydning når det gjelder å bygge opp tillit blant markedsdeltakere, ettersom de viser at tjenestetilbyderen har status som kvalifisert på tidspunktet for tilsynet.

47) Tillit til og brukervennlighet i forbindelse med nettbaserte tjenester er avgjørende for at brukerne skal kunne ha fullt utbytte av og vite at de kan stole på elektroniske tjenester. Det bør derfor innføres et EU-tillitsmerke for å identifisere de kvalifiserte tillitstjenestene som leveres av kvalifiserte tilbydere av tillitstjenester. Et slikt EU-tillitsmerke for kvalifiserte tillitstjenester vil gjøre det mulig å tydelig skille mellom kvalifiserte tillitstjenester og andre tillitstjenester og dermed bidra til oversikt i markedet. Det bør være frivillig for kvalifiserte tilbydere av tillitstjenester å bruke et EU-tillitsmerke, og dette bør ikke medføre andre krav enn dem som er fastsatt i denne forordning.

48) Det kreves et høyt sikkerhetsnivå for å sikre gjensidig anerkjennelse av elektroniske signaturer, men i særlige tilfeller, for eksempel innenfor rammen av kommisjonsvedtak 2009/767/EF([1]), bør elektroniske signaturer med et lavere sikkerhetsnivå også godtas.

49) Denne forordning bør fastsette prinsippet om at en elektronisk signatur ikke bør nektes rettsvirkning med den begrunnelse at den er elektronisk, eller at den ikke oppfyller kravene til en kvalifisert elektronisk signatur. Elektroniske signaturers rettsvirkning skal imidlertid fastsettes i nasjonal lovgivning, bortsett fra kravene fastsatt i denne forordning om at en kvalifisert elektronisk signatur skal ha samme rettsvirkning som en håndskreven signatur.

50) Ettersom vedkommende myndigheter i medlemsstatene i dag benytter forskjellige formater for avanserte elektroniske signaturer til å signere sine dokumenter elektronisk, må det sikres at i det minste et visst antall formater for avanserte elektroniske signaturer kan støttes teknisk av medlemsstatene når de mottar dokumenter som er signert elektronisk. Når vedkommende myndigheter i medlemsstatene benytter avanserte elektroniske segl, må det også sikres at de i det minste støtter et visst antall formater for avanserte elektroniske segl.

51) Det bør være mulig for underskriveren å overlate ansvaret for kvalifiserte elektroniske signaturframstillingssystemer til en tredjepart, forutsatt at det finnes egnede ordninger og framgangsmåter som sikrer at underskriveren har enekontroll over bruken av sine data til framstilling av elektroniske signaturer, og at bruken av systemet oppfyller kravene til kvalifiserte elektroniske signaturer.

52) Fjernframstilling av elektroniske signaturer, der miljøet for framstilling av elektroniske signaturer forvaltes av en tilbyder av tillitstjenester på vegne av underskriveren, forventes å øke i omfang på grunn av de mange økonomiske fordelene dette innebærer. For å sikre at slike elektroniske signaturer oppnår den samme rettslige anerkjennelse som elektroniske signaturer framstilt i et miljø som helt og holdent forvaltes av brukeren, skal tjenestetilbydere som tilbyr fjerntjenester for elektroniske signaturer, imidlertid anvende særlige forvaltningsmessige og administrative sikkerhetsprosedyrer og benytte pålitelige systemer og produkter, herunder sikre elektroniske kommunikasjonskanaler, for å sikre at miljøet for framstilling av elektroniske signaturer er pålitelig og at underskriveren har enekontroll over bruken av det. Dersom en kvalifisert elektronisk signatur er blitt framstilt ved hjelp av et system for fjernframstilling av elektroniske signaturer, får kravene som gjelder for kvalifiserte tilbydere av tillitstjenester fastsatt i denne forordning, anvendelse.

53) Midlertidig oppheving av kvalifiserte sertifikater er en etablert praksis blant tilbydere av tillitstjenester i en rekke medlemsstater som ikke er det samme som tilbakekalling, og som innebærer et midlertidig tap av et sertifikats gyldighet. Av hensyn til rettssikkerheten kreves det at sertifikatets opphevingsstatus alltid angis tydelig. Tilbydere av tillitstjenester bør derfor ha ansvar for tydelig å angi sertifikatets status og, dersom det er midlertidig opphevet, det nøyaktige tidsrommet der sertifikatet er opphevet. Ved denne forordning bør tilbydere av tillitstjenester eller medlemsstater ikke pålegges å benytte midlertidig oppheving, men det bør fastsettes regler for innsyn dersom en slik praksis er tilgjengelig.

54) Samvirkingsevne og anerkjennelse over landegrensene av kvalifiserte sertifikater er en forutsetning for anerkjennelse over landegrensene av kvalifiserte elektroniske signaturer. Kvalifiserte sertifikater bør derfor ikke omfattes av ufravikelige krav som går lenger enn kravene fastsatt i denne forordning. På nasjonalt plan bør det imidlertid være tillatt å ta med særlige attributter, for eksempel entydige

1. Kommisjonsvedtak 2009/767/EF av 16. oktober 2009 om fastsettelse av tiltak for å forenkle bruken av elektroniske framgangsmåter ved hjelp av «felles kontaktpunkter» i samsvar med europaparlaments- og rådsdirektiv 2006/123/EF om tjenester i det indre marked (EUT L 274 av 20.10.2009, s. 36)

identifikatorer, i kvalifiserte sertifikater, forutsatt at slike særlige attributter ikke hindrer samvirkingsevne og anerkjennelse over landegrensene av kvalifiserte sertifikater og elektroniske signaturer.

55) IT-sikkerhetssertifisering som bygger på internasjonale standarder som ISO 15408 og tilknyttede vurderingsmetoder og ordninger for gjensidig anerkjennelse, er et viktig verktøy for å kontrollere sikkerheten i kvalifiserte elektroniske signaturframstillingssystemer, og bør fremmes. Nyskapende løsninger og tjenester, for eksempel signering via mobiltelefon og via nettskyen, krever tekniske og organisatoriske løsninger for kvalifiserte elektroniske signaturframstillingssystemer som det foreløpig kanskje ikke finnes tilgjengelige sikkerhetsstandarder for, eller der den første IT-sikkerhetssertifiseringen ikke er avsluttet. Sikkerhetsnivået for slike kvalifiserte elektroniske signaturframstillingssystemer kan vurderes ved hjelp av alternative prosesser bare dersom slike sikkerhetsstandarder ikke er tilgjengelige, eller dersom den første IT-sikkerhetssertifiseringen ikke er avsluttet. Prosessene bør være sammenlignbare med standardene for IT-sikkerhetssertifisering i den grad sikkerhetsnivåene er de samme. En fagfellevurdering vil kunne fremme disse prosessene.

56) Ved denne forordning bør det fastsettes krav til kvalifiserte elektroniske signaturframstillingssystemer for å sikre at avanserte elektroniske signaturer fungerer hensiktsmessig. Denne forordning bør ikke omfatte hele systemmiljøet der slike systemer benyttes. Omfanget av sertifiseringen av kvalifiserte signaturframstillingssystemer bør derfor begrenses til maskinvaren og systemprogramvaren som brukes til håndtering og vern av signaturframstillingsdataene som framstilles, lagres eller behandles i signaturframstillingssystemet. Som angitt i relevante standarder bør sertifiseringsplikten ikke omfatte signaturframstillingsprogrammer.

57) For å ivareta rettssikkerheten med hensyn til signaturens gyldighet er det viktig å angi hvilke elementer av en kvalifisert elektronisk signatur som bør vurderes av tjenestebrukeren som utfører valideringen. En fastsettelse av kravene til kvalifiserte tilbydere av tillitstjenester som kan tilby en kvalifisert valideringstjeneste til tjenestebrukere som ikke er villige eller i stand til selv å utføre valideringen av kvalifiserte elektroniske signaturer, bør dessuten stimulere privat og offentlig sektor til å investere i slike tjenester. Begge elementene bør gjøre det enkelt og praktisk å validere kvalifiserte elektroniske signaturer for alle parter på EU-plan.

58) Dersom en transaksjon krever et kvalifisert elektronisk segl fra en juridisk person, bør en kvalifisert elektronisk signatur fra den juridiske personens godkjente representant også godkjennes.

59) Elektroniske segl bør tjene som bevis på at et elektronisk dokument er utstedt av en juridisk person, og gi en garanti for dokumentets opprinnelse og integritet.

60) Tilbydere av tillitstjenester som utsteder kvalifiserte sertifikater for elektroniske segl, bør treffe nødvendige tiltak for å kunne fastslå identiteten til den fysiske personen som representerer den juridiske personen som det kvalifiserte sertifikatet for det elektroniske seglet utstedes til, dersom slik identifikasjon er nødvendig på nasjonalt plan som ledd i en rettergang eller en forvaltningssak.

61) Denne forordning bør sikre langsiktig bevaring av opplysninger for å sikre at elektroniske signaturer og elektroniske segl har rettslig gyldighet i lengre perioder og kan valideres uavhengig av framtidige teknologiske endringer.

62) For å garantere sikkerheten til kvalifiserte elektroniske tidsstempler bør det ved denne forordning kreves at det benyttes et avansert elektronisk segl eller en avansert elektronisk signatur eller andre tilsvarende metoder. Nyskaping vil trolig føre til ny teknologi som kan sikre et tilsvarende sikkerhetsnivå for tidsstempler. Dersom det benyttes en annen metode enn et avansert elektronisk segl eller en avansert elektronisk signatur, bør det være opp til den kvalifiserte tilbyderen av tillitstjenester å vise i samsvarsvurderingsrapporten at metoden sikrer et tilsvarende sikkerhetsnivå og oppfyller kravene fastsatt i denne forordning.

63) Elektroniske dokumenter er viktig for den videre utviklingen av elektroniske transaksjoner over landegrensene i det indre marked. Denne forordning bør fastsette prinsippet om at et elektronisk dokument ikke bør nektes rettsvirkning med den begrunnelse at det er elektronisk, for å sikre at en elektronisk transaksjon ikke vil bli avvist alene fordi et dokument foreligger i elektronisk form.

64) Når Kommisjonen behandler spørsmålet om formater for avanserte elektroniske signaturer og segl, bør den ta utgangspunkt i eksisterende praksis, standarder og regelverk, særlig kommisjonsbeslutning 2011/130/EU([1]).

65) I tillegg til å autentisere et dokument utstedt av en juridisk person kan elektroniske segl benyttes til å autentisere en juridisk persons digitale eiendeler, for eksempel programvarekode eller tjenere.

1. Kommisjonsbeslutning 2011/130/EU av 25. februar 2011 om fastsettelse av minstekrav til behandling over landegrensene av dokumenter som signeres elektronisk av vedkommende myndigheter i henhold til europaparlaments- og rådsdirektiv 2006/123/EF om tjenester i det indre marked (EUT L 53 av 26.2.2011, s. 66)

66) Det er svært viktig å fastsette en rettslig ramme for å fremme anerkjennelse over landegrensene mellom eksisterende nasjonale rettsordener for elektroniske tjenester for registrert sending. Rammen kan også gi nye avsetningsmuligheter som vil gjøre det mulig for tilbydere av tillitstjenester i Unionen å tilby nye felleseuropeiske elektroniske tjenester for registrert sending.

67) Nettstedsautentiseringstjenester gir besøkende på et nettsted sikkerhet for at det bak nettstedet står en ekte og rettmessig enhet. Slike tjenester bidrar til å bygge opp tilliten til forretningsvirksomhet på nettet, ettersom brukerne vil ha tillit til et nettsted som er blitt autentisert. Levering og bruk av nettstedsautentiseringstjenester er helt og holdent frivillig. For at nettstedsautentisering skal bli et middel for å styrke tilliten, gi en bedre opplevelse for brukeren og fremme veksten i det indre marked, bør det ved denne forordning fastsettes minstekrav til sikkerhet og erstatningsansvar for tjenestetilbyderne og deres tjenester. I denne forbindelse er det tatt hensyn til resultatene fra eksisterende initiativer ledet av industrien, for eksempel «Certification Authorities/ Browsers Forum – CA/B Forum». Denne forordning bør heller ikke hindre bruk av andre midler eller metoder for autentisering av et nettsted som ikke omfattes av denne forordning, eller hindre tilbydere av nettstedsautentiseringstjenester i tredjestater i å tilby sine tjenester til kunder i Unionen. En tjenestetilbyder i en tredjestat bør imidlertid kunne få sine nettstedsautentiseringstjenester anerkjent som kvalifiserte i samsvar med denne forordning bare dersom det er inngått en internasjonal avtale mellom Unionen og den staten der tjenestetilbyderen er etablert.

68) I henhold til bestemmelsene om etablering i traktaten om Den europeiske unions virkemåte (TEUV) gir begrepet «juridiske personer» markedsdeltakere mulighet til fritt å velge hvilken juridisk form de anser som egnet for å utøve sin virksomhet. Følgelig er «juridiske personer» i henhold til TEUV alle foretak som er opprettet i henhold til, eller underlagt, lovgivningen i en medlemsstat, uansett juridisk form.

69) I forbindelse med forvaltningssamarbeid oppfordres Unionens institusjoner, organer, kontorer og byråer til å anerkjenne elektronisk identifikasjon og tillitstjenester som omfattes av denne forordning, særlig for å dra nytte av eksisterende god praksis og resultatene fra pågående prosjekter på områder som omfattes av denne forordning.

70) For å utfylle visse detaljerte tekniske aspekter ved denne forordning på en fleksibel og rask måte bør myndigheten til å vedta rettsakter i samsvar med artikkel 290 i TEUV delegeres til Kommisjonen med tanke på de kriterier som skal oppfylles av organer med ansvar for sertifisering av kvalifiserte elektroniske signaturframstillingssystemer. Det er særlig viktig at Kommisjonen holder hensiktsmessige samråd under sitt forberedende arbeid, herunder på ekspertnivå. Kommisjonen bør ved forberedelse og utarbeiding av delegerte rettsakter sikre at relevante dokumenter oversendes Europaparlamentet og Rådet samtidig, til rett tid og på en egnet måte.

71) For å sikre ensartede vilkår for gjennomføring av denne forordning bør Kommisjonen gis gjennomføringsmyndighet, særlig når det gjelder å angi referansenumre for standarder hvis bruk vil skape en formodning om samsvar med visse bestemmelser fastsatt i denne forordning. Denne myndighet bør utøves i samsvar med europaparlaments- og rådsforordning (EU) nr. 182/2011([1]).

72) Når Kommisjonen vedtar delegerte rettsakter eller gjennomføringsrettsakter, bør den ta behørig hensyn til standarder og tekniske spesifikasjoner utarbeidet av europeiske og internasjonale standardiseringsorganisasjoner og -organer, særlig Den europeiske standardiseringsorganisasjon (CEN), Det europeiske standardiseringsinstitutt for telekommunikasjon (ETSI), Den internasjonale standardiseringsorganisasjon (ISO) og Den internasjonale teleunion (ITU), for å sikre et høyt nivå av sikkerhet og samvirkingsevne i forbindelse med elektronisk identifikasjon og tillitstjenester.

73) Av rettssikkerhets- og klarhetshensyn bør direktiv 1999/93/EF oppheves.

74) For å ivareta rettssikkerheten for markedsdeltakere som allerede benytter kvalifiserte sertifikater utstedt til fysiske personer i samsvar med direktiv 1999/93/EF, må det fastsettes en tilstrekkelig lang overgangsperiode. Det bør også fastsettes overgangstiltak for sikre signaturframstillingssystemer hvis samsvar er blitt fastslått i samsvar med direktiv 1999/93/EF, samt for tilbydere av sertifiseringstjenester som utsteder kvalifiserte sertifikater før 1. juli 2016. Det er også nødvendig å gi Kommisjonen mulighet til å vedta gjennomføringsrettsaktene og de delegerte rettsaktene før nevnte dato.

75) Anvendelsesdatoene fastsatt i denne forordning berører ikke eksisterende forpliktelser som medlemsstatene allerede har i henhold til unionsretten, særlig i henhold til direktiv 2006/123/EF.

76) Ettersom målene for denne forordning ikke kan nås i tilstrekkelig grad av medlemsstatene og derfor på grunn av tiltakets omfang bedre kan nås på unionsplan, kan Unionen treffe tiltak i samsvar med nær-

1. Europaparlaments- og rådsforordning (EU) nr. 182/2011 av 16. februar 2011 om fastsettelse av allmenne regler og prinsipper for medlemsstatenes kontroll med Kommisjonens utøvelse av sin gjennomføringsmyndighet (EUT L 55 av 28.2.2011, s. 13).

hetsprinsippet som fastsatt i artikkel 5 i traktaten om Den europeiske union. I samsvar med forholdsmessighetsprinsippet fastsatt i nevnte artikkel går denne forordning ikke lenger enn det som er nødvendig for å nå disse målene.

77) EUs datatilsynsmann er blitt rådspurt i samsvar med artikkel 28 nr. 2 i europaparlaments- og rådsforordning (EF) nr. 45/2001([1]) og avga uttalelse 27. september 2012([2]) —

VEDTATT DENNE FORORDNING:

KAPITTEL I

ALMINNELIGE BESTEMMELSER

Artikkel 1

Formål

For å sikre at det indre marked fungerer på en tilfredsstillende måte, og for å oppnå et egnet sikkerhetsnivå for elektroniske identifikasjonsmidler og tillitstjenester er formålet med denne forordning å

a) fastsette vilkårene for medlemsstatenes anerkjennelse av midler for elektronisk identifikasjon av fysiske og juridiske personer som omfattes av en meldt ordning for elektronisk identifikasjon i en annen medlemsstat,
b) fastsette regler for tillitstjenester, særlig for elektroniske transaksjoner, og
c) fastsette en rettslig ramme for elektroniske signaturer, elektroniske segl, elektroniske tidsstempler, elektroniske dokumenter, elektroniske tjenester for registrert sending og sertifikattjenester for nettstedsautentisering.

Artikkel 2

Virkeområde

1. Denne forordning får anvendelse på ordninger for elektronisk identifikasjon som er meldt av en medlemsstat, og på tilbydere av tillitstjenester som er etablert i Unionen.
2. Denne forordning får ikke anvendelse på tillitstjenester som utelukkende benyttes i lukkede systemer som følge av nasjonal lovgivning eller avtaler mellom en definert gruppe av deltakere.
3. Denne forordning berører ikke nasjonal lovgivning eller unionsretten som gjelder inngåelse av kontrakter eller kontrakters gyldighet eller andre formelle juridiske eller prosedyremessige forpliktelser med hensyn til formkrav.

Artikkel 3

Definisjoner

I denne forordning menes med:

1) «elektronisk identifikasjon» en prosess som omfatter bruk av personidentifikasjonsdata i elektronisk form som på en entydig måte representerer enten en fysisk eller juridisk person, eller en fysisk person som representerer en juridisk person,
2) «elektronisk identifikasjonsmiddel» en materiell og/eller immateriell enhet som inneholder personidentifikasjonsdata, og som brukes til autentisering av en nettbasert tjeneste,
3) «personidentifikasjonsdata» et datasett som gjør det mulig å fastslå identiteten til en fysisk eller juridisk person, eller en fysisk person som representerer en juridisk person,
4) «ordning for elektronisk identifikasjon» et system for elektronisk identifikasjon der det utstedes elektroniske identifikasjonsmidler til fysiske eller juridiske personer, eller til fysiske personer som representerer juridiske personer,
5) «autentisering» en elektronisk prosess som gjør det mulig å bekrefte den elektroniske identifikasjonen av en fysisk eller juridisk person, eller opprinnelsen og integriteten til data i elektronisk form,
6) «tjenestebruker» en fysisk eller juridisk person som benytter seg av elektronisk identifikasjon eller en tillitstjeneste,
7) «offentlig organ» en statlig, regional eller lokal myndighet, et offentligrettslig organ eller en sammenslutning av én eller flere av nevnte myndigheter eller ett eller flere av nevnte offentligrettslige organer, eller en privat enhet med mandat fra minst én av nevnte myndigheter, organer eller sammenslutninger til å tilby offentlige tjenester, når den opptrer i henhold til et slikt mandat,
8) «offentligrettslig organ» et organ som definert i artikkel 2 nr. 1 punkt 4 i europaparlaments- og rådsdirektiv 2014/24/EU([3]),
9) «underskriver» en fysisk person som framstiller en elektronisk signatur,
10) «elektronisk signatur» data i elektronisk form som er lagt ved eller er logisk knyttet til andre data i elektronisk form, og som underskriveren bruker til å signere,
11) «avansert elektronisk signatur» en elektronisk signatur som oppfyller kravene fastsatt i artikkel 26,

1. Europaparlaments- og rådsforordning (EF) nr. 45/2001 av 18. desember 2000 om personvern i forbindelse med behandling av personopplysninger i Fellesskapets institusjoner og organer og om fri utveksling av slike opplysninger (EFT L 8 av 12.1.2001, s. 1).
2. EUT C 28 av 30.1.2013, s. 6.
3. Europaparlaments- og rådsdirektiv 2014/24/EU av 26. februar 2014 om offentlige innkjøp og om oppheving av direktiv 2004/18/EF (EUT L 94 av 28.3.2014, s. 65).

12) «kvalifisert elektronisk signatur» en avansert elektronisk signatur som er framstilt ved hjelp av et kvalifisert elektronisk signaturframstillingssystem, og som bygger på et kvalifisert sertifikat for elektroniske signaturer,
13) «elektroniske signaturframstillingsdata» entydige data som underskriveren bruker til å framstille en elektronisk signatur,
14) «sertifikat for elektronisk signatur» en elektronisk attest som knytter valideringsdata for en elektronisk signatur til en fysisk person og minst bekrefter denne personens navn eller pseudonym,
15) «kvalifisert sertifikat for elektronisk signatur» et sertifikat for elektroniske signaturer som er utstedt av en kvalifisert tilbyder av tillitstjenester, og som oppfyller kravene fastsatt i vedlegg I,
16) «tillitstjeneste» en elektronisk tjeneste som normalt tilbys mot betaling, og som består av
    a) framstilling, kontroll og validering av elektroniske signaturer, elektroniske segl eller elektroniske tidsstempler, elektroniske tjenester for registrert sending og sertifikater knyttet til slike tjenester eller
    b) framstilling, kontroll og validering av sertifikater for nettstedsautentisering eller
    c) bevaring av elektroniske signaturer, segl eller sertifikater knyttet til slike tjenester,
17) «kvalifisert tillitstjeneste» en tillitstjeneste som oppfyller gjeldende krav fastsatt i denne forordning,
18) «samsvarsvurderingsorgan» et organ som definert i artikkel 2 nr. 13 i forordning (EF) nr. 765/2008, som er akkreditert i samsvar med nevnte forordning som kompetent til å utføre samsvarsvurdering av en kvalifisert tilbyder av tillitstjenester og de kvalifiserte tillitstjenestene denne leverer,
19) «tilbyder av tillitstjenester» en fysisk eller juridisk person som leverer en eller flere tillitstjenester som tilbyder av enten kvalifiserte eller ikke-kvalifiserte tillitstjenester,
20) «kvalifisert tilbyder av tillitstjenester» en tilbyder av tillitstjenester som leverer en eller flere kvalifiserte tillitstjenester, og som har fått tildelt status som kvalifisert av tilsynsorganet,
21) «produkt» maskinvare eller programvare, eller relevante maskin- eller programvarekomponenter, beregnet på bruk i forbindelse med levering av tillitstjenester,
22) «elektronisk signaturframstillingssystem» konfigurert programvare eller maskinvare som brukes til framstilling av en elektronisk signatur,
23) «kvalifisert elektronisk signaturframstillingssystem» et elektronisk signaturframstillingssystem som oppfyller kravene fastsatt i vedlegg II,
24) «seglframstiller» en juridisk person som framstiller et juridisk segl,
25) «elektronisk segl» data i elektronisk form som er lagt ved eller er logisk knyttet til andre data i elektronisk form for å sikre sistnevntes opprinnelse og integritet,
26) «avansert elektronisk segl» et elektronisk segl som oppfyller kravene i artikkel 36,
27) «kvalifisert elektronisk segl» et avansert elektronisk segl som er framstilt ved hjelp av et kvalifisert elektronisk seglframstillingssystem, og som bygger på et kvalifisert sertifikat for elektroniske segl,
28) «elektroniske seglframstillingsdata» entydige data som framstilleren av det elektroniske seglet bruker til å framstille et elektronisk segl,
29) «sertifikat for elektronisk segl» en elektronisk attest som knytter valideringsdata for et elektronisk segl til en juridisk person og bekrefter denne personens navn,
30) «kvalifisert sertifikat for elektronisk segl» et sertifikat for et elektronisk segl som er utstedt av en kvalifisert tilbyder av tillitstjenester, og som oppfyller kravene fastsatt i vedlegg III,
31) «elektronisk seglframstillingssystem» konfigurert programvare eller maskinvare som brukes til framstilling av et elektronisk segl,
32) «kvalifisert elektronisk seglframstillingssystem» et elektronisk seglframstillingssystem som med de nødvendige endringer oppfyller kravene fastsatt i vedlegg II,
33) «elektronisk tidsstempel» data i elektronisk form som knytter andre data i elektronisk form til et bestemt tidspunkt og dokumenterer at sistnevnte data eksisterte på det tidspunktet,
34) «kvalifisert elektronisk tidsstempel» et elektronisk tidsstempel som oppfyller kravene i artikkel 42,
35) «elektronisk dokument» innhold lagret i elektronisk form, særlig tekst, lyd, bilder eller audiovisuelle opptak,
36) «elektronisk tjeneste for registrert sending» en tjeneste som gjør det mulig å overføre data elektronisk mellom tredjeparter, som omfatter dokumentasjon av håndteringen av de overførte dataene, herunder dokumentasjon av sending og mottak av dataene, og som beskytter overførte data mot tap, tyveri, skade eller ikke-autoriserte endringer,
37) «kvalifisert elektronisk tjeneste for registrert sending» en elektronisk tjeneste for registrert sending som oppfyller kravene fastsatt i artikkel 44,
38) «sertifikat for nettstedsautentisering» en attest som gjør det mulig å autentisere et nettsted, og som knytter nettstedet til den fysiske eller juridiske personen som sertifikatet er utstedt til,
39) «kvalifisert sertifikat for nettstedsautentisering» et sertifikat for nettstedsautentisering som er utstedt

av en kvalifisert tilbyder av tillitstjenester, og som oppfyller kravene fastsatt i vedlegg IV,

40) «valideringsdata» data som brukes til validering av en elektronisk signatur eller et elektronisk segl,

41) «validering» prosessen med å kontrollere og bekrefte at en elektronisk signatur eller et elektronisk segl er gyldig.

ARTIKKEL 4

PRINSIPPET OM DET INDRE MARKED

1. En tilbyder av tillitstjenester som er etablert i en medlemsstat, skal ikke bli gjenstand for begrensning på levering av tillitstjenester på territoriet til en annen medlemsstat av årsaker som faller inn under områdene som omfattes av denne forordning.
2. Produkter og tillitstjenester som oppfyller kravene i denne forordning, skal omfattes av fri bevegelighet i det indre marked.

ARTIKKEL 5

BEHANDLING OG VERN AV PERSONOPPLYSNINGER

1. Personopplysninger skal behandles i samsvar med direktiv 95/46/EF.
2. Med forbehold for den rettsvirkning som pseudonymer er gitt i henhold til nasjonal lovgivning, skal bruk av pseudonymer i elektroniske transaksjoner ikke forbys.

KAPITTEL II

ELEKTRONISK IDENTIFIKASJON

ARTIKKEL 6

GJENSIDIG ANERKJENNELSE

1. Dersom det i henhold til nasjonal lovgivning eller forvaltningspraksis kreves elektronisk identifikasjon ved hjelp av et elektronisk identifikasjonsmiddel samt autentisering for å få tilgang til en nettbasert tjeneste som leveres av et offentlig organ i en medlemsstat, skal det elektroniske identifikasjonsmiddelet utstedt i en annen medlemsstat anerkjennes i den første medlemsstaten med henblikk på autentisering over landegrensene av den nettbaserte tjenesten, forutsatt at følgende vilkår er oppfylt:
   a) det elektroniske identifikasjonsmiddelet er utstedt innenfor rammen av en ordning for elektronisk identifikasjon som er oppført på listen offentliggjort av Kommisjonen i henhold til artikkel 9,
   b) sikkerhetsnivået for det elektroniske identifikasjonsmiddelet tilsvarer eller er høyere enn sikkerhetsnivået som kreves av det berørte offentlige organet for å få tilgang til den nettbaserte tjenesten i den første medlemsstaten, forutsatt at sikkerhetsnivået for det elektroniske identifikasjonsmiddelet tilsvarer sikkerhetsnivået «betydelig» eller «høyt»,
   c) det berørte offentlige organet benytter sikkerhetsnivået «betydelig» eller «høyt» i forbindelse med tilgang til den nettbaserte tjenesten.

Anerkjennelsen skal finne sted senest tolv måneder etter at Kommisjonen har offentliggjort listen nevnt i nr. 1 bokstav a).

2. Et elektronisk identifikasjonsmiddel som utstedes innenfor rammen av en ordning for elektronisk identifikasjon som er oppført på listen offentliggjort av Kommisjonen i henhold til artikkel 9, og som tilsvarer sikkerhetsnivået «lavt», kan anerkjennes av offentlige organer med henblikk på autentisering over landegrensene av den nettbaserte tjenesten som organene tilbyr.

ARTIKKEL 7

MELDING AV ORDNINGER FOR ELEKTRONISK IDENTIFIKASJON

En ordning for elektronisk identifikasjon kan meldes i henhold til artikkel 9 nr. 1 dersom alle vilkårene nedenfor er oppfylt:

a) det elektroniske identifikasjonsmiddelet innenfor rammen av ordningen for elektronisk identifikasjon er utstedt
   i) av meldermedlemsstaten,
   ii) i henhold til et mandat fra meldermedlemsstaten eller
   iii) uavhengig av meldermedlemsstaten og er anerkjent av nevnte medlemsstat,
b) det elektroniske identifikasjonsmiddelet innenfor rammen av ordningen for elektronisk identifikasjon kan brukes for å få tilgang til minst én tjeneste som tilbys av et offentlig organ, og som krever elektronisk identifikasjon i meldermedlemsstaten,
c) ordningen for elektronisk identifikasjon og det elektroniske identifikasjonsmiddelet utstedt innenfor rammen av ordningen, oppfyller kravene til minst ett av sikkerhetsnivåene fastsatt i gjennomføringsrettsakten nevnt i artikkel 8 nr. 3,
d) meldermedlemsstaten sikrer at personidentifikasjonsdataene som på en entydig måte representerer den aktuelle personen, i samsvar med de tekniske spesifikasjonene, standardene og framgangsmåtene for det relevante sikkerhetsnivået fastsatt i gjennomføringsrettsakten nevnt i artikkel 8 nr. 3,

knyttes til den fysiske eller juridiske personen nevnt i artikkel 3 nr. 1 på tidspunktet for utstedelse av det elektroniske identifikasjonsmiddelet innenfor rammen av nevnte ordning,

e) parten som utsteder det elektroniske identifikasjonsmiddelet innenfor rammen av nevnte ordning, sikrer at det elektroniske identifikasjonsmiddelet knyttes til personen nevnt i bokstav d) i denne artikkel i samsvar med de tekniske spesifikasjonene, standardene og framgangsmåtene for det relevante sikkerhetsnivået fastsatt i gjennomføringsrettsakten nevnt i artikkel 8 nr. 3,

f) meldermedlemsstaten sikrer at autentisering via internett er tilgjengelig, slik at tjenestebrukere som er etablert på en annen medlemsstats territorium, kan bekrefte personidentifikasjonsdataene som er mottatt i elektronisk form.

For andre tjenestebrukere enn offentlige organer kan meldermedlemsstaten definere vilkår for tilgang til autentiseringen. Autentisering over landegrensene skal være gratis når det utføres i forbindelse med en nettbasert tjeneste som tilbys av et offentlig organ.

Medlemsstatene skal ikke pålegge tjenestebrukere som har til hensikt å utføre en slik autentisering, urimelige tekniske krav, dersom slike krav hindrer eller i vesentlig grad hemmer samvirkingsevnen til de meldte ordningene for elektronisk identifikasjon,

g) minst seks måneder før det gis melding i henhold til artikkel 9 nr. 1 skal meldermedlemsstaten, med tanke på forpliktelsen nevnt i artikkel 12 nr. 5, gi de andre medlemsstatene en beskrivelse av ordningen i samsvar med saksbehandlingsreglene fastsatt ved gjennomføringsrettsaktene nevnt i artikkel 12 nr. 7,

h) ordningen for elektronisk identifikasjon oppfyller kravene fastsatt i gjennomføringsrettsaktene nevnt i artikkel 12 nr. 8.

Artikkel 8

Sikkerhetsnivåer for ordninger for elektronisk identifikasjon

1. I en ordning for elektronisk identifikasjon som er meldt i henhold til artikkel 9 nr. 1, skal sikkerhetsnivåene «lavt», «betydelig» og/eller «høyt» angis for elektroniske identifikasjonsmidler utstedt innenfor rammen av denne ordningen.
2. Sikkerhetsnivåene «lavt», «betydelig» og «høyt» skal oppfylle følgende kriterier:
   a) sikkerhetsnivået «lavt» skal vise til et elektronisk identifikasjonsmiddel innenfor rammen av en ordning for elektronisk identifikasjon som gir en begrenset grad av tillit til en persons påberopte eller påståtte identitet, og som kjennetegnes på grunnlag av tekniske spesifikasjoner, standarder og framgangsmåter knyttet til dette, herunder tekniske kontroller, hvis formål er å redusere risikoen for misbruk eller endring av identiteten,
   b) sikkerhetsnivået «betydelig» skal vise til et elektronisk identifikasjonsmiddel innenfor rammen av en ordning for elektronisk identifikasjon som gir en betydelig grad av tillit til en persons påberopte eller påståtte identitet, og som kjennetegnes på grunnlag av tekniske spesifikasjoner, standarder og framgangsmåter knyttet til dette, herunder tekniske kontroller, hvis formål er å oppnå en betydelig redusert risiko for misbruk eller endring av identiteten,
   c) sikkerhetsnivået «høyt» skal vise til et elektronisk identifikasjonsmiddel innenfor rammen av en ordning for elektronisk identifikasjon som gir en høyere grad av tillit til en persons påberopte eller påståtte identitet enn elektroniske identifikasjonsmidler med sikkerhetsnivået «betydelig», og som kjennetegnes på grunnlag av tekniske spesifikasjoner, standarder og framgangsmåter knyttet til dette, herunder tekniske kontroller, hvis formål er å hindre misbruk eller endring av identiteten,
3. Innen 18. september 2015 skal Kommisjonen, idet det tas hensyn til relevante internasjonale standarder og med forbehold for nr. 2, ved hjelp av gjennomføringsrettsakter fastsette tekniske minstespesifikasjoner, minstestandarder og minstekrav til framgangsmåter som skal utgjøre grunnlaget for angivelse av sikkerhetsnivåene «lavt», «betydelig» og «høyt» for elektroniske identifikasjonsmidler med henblikk på nr. 1.

Disse tekniske minstespesifikasjonene, minstestandardene og minstekravene til framgangsmåter skal fastsettes med henvisning til følgende elementers pålitelighet og kvalitet:

a) framgangsmåten for å bevise og kontrollere identiteten til fysiske eller juridiske personer som søker om utstedelse av elektroniske identifikasjonsmidler,

b) framgangsmåten for utstedelse av de elektroniske identifikasjonsmidlene som det er anmodet om,

c) autentiseringsordningen som gjør det mulig for den fysiske eller juridiske personen å bruke det elektroniske identifikasjonsmiddelet til å bekrefte sin identitet overfor en tjenestebruker,

d) enheten som utsteder de elektroniske identifikasjonsmidlene,

e) ethvert annet organ involvert i søknaden om utstedelse av elektroniske identifikasjonsmidler og

f) de tekniske spesifikasjonene og sikkerhetsspesifikasjonene for de utstedte elektroniske identifikasjonsmidlene.

Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

ARTIKKEL 9

MELDING

1. Meldermedlemsstaten skal gi Kommisjonen følgende opplysninger og så snart som mulig underrette om eventuelle endringer av dem:
   a) en beskrivelse av ordningen for elektronisk identifikasjon, herunder ordningens sikkerhetsnivåer og utstederen/utstederne av elektroniske identifikasjonsmidler innenfor rammen av ordningen,
   b) den gjeldende tilsynsordningen og opplysninger om ansvarsordningen med hensyn til følgende:
      i) parten som utsteder det elektroniske identifikasjonsmiddelet, og
      ii) parten som utfører framgangsmåten for autentisering,
   c) myndigheten(e) som har ansvar for ordningen for elektronisk identifikasjon,
   d) opplysninger om enheten(e) som tar hånd om registreringen av de entydige personidentifikasjonsdataene,
   e) en beskrivelse av hvordan kravene fastsatt i gjennomføringsrettsaktene nevnt i artikkel 12 nr. 8 er oppfylt,
   f) en beskrivelse av autentiseringen nevnt i artikkel 7 bokstav f),
   g) ordninger for midlertidig oppheving eller tilbakekalling av enten den meldte ordningen for elektronisk identifikasjon, autentiseringen eller de berørte utsatte delene.
2. Ett år fra anvendelsesdatoen for gjennomføringsrettsaktene nevnt i artikkel 8 nr. 3 og 12 nr. 8 skal Kommisjonen offentliggjøre en liste over ordningene for elektronisk identifikasjon meldt i henhold til nr. 1 i denne artikkel samt de grunnleggende opplysningene om disse i *Den europeiske unions tidende*.
3. Dersom Kommisjonen mottar en melding etter utgangen av perioden nevnt i nr. 2, skal den offentliggjøre endringene som er gjort i listen nevnt i nr. 2, i *Den europeiske unions tidende* innen to måneder etter datoen for mottak av meldingen.
4. En medlemsstat kan anmode Kommisjonen om å fjerne en ordning for elektronisk identifikasjon som er meldt av medlemsstaten, fra listen nevnt i nr. 2. Kommisjonen skal offentliggjøre de aktuelle endringene som er gjort i listen, i *Den europeiske unions tidende* innen én måned etter datoen for mottak av medlemsstatens anmodning.
5. Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette vilkår, formater og framgangsmåter for meldingene nevnt i nr. 1. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

ARTIKKEL 10

SIKKERHETSBRUDD

1. Dersom enten ordningen for elektronisk identifikasjon meldt i henhold til artikkel 9 nr. 1 eller autentiseringen nevnt i artikkel 7 bokstav f) utsettes for et brudd eller en delvis svekkelse på en måte som påvirker påliteligheten til ordningens autentisering over landegrensene, skal meldermedlemsstaten omgående midlertidig oppheve eller tilbakekalle denne autentiseringen over landegrensene eller de berørte svekkede delene og underrette andre medlemsstater og Kommisjonen.
2. Dersom bruddet eller svekkelsen nevnt i nr. 1 utbedres, skal meldermedlemsstaten gjenopprette autentiseringen over landegrensene og underrette andre medlemsstater og Kommisjonen så snart som mulig.
3. Dersom bruddet eller svekkelsen nevnt i nr. 1 ikke utbedres innen tre måneder etter den midlertidige opphevingen eller tilbakekallingen, skal meldermedlemsstaten underrette andre medlemsstater og Kommisjonen om at ordningen for elektronisk identifikasjon er trukket tilbake.

Kommisjonen skal så snart som mulig offentliggjøre de tilsvarende endringene som er gjort i listen nevnt i artikkel 9 nr. 2, i Den europeiske unions tidende.

ARTIKKEL 11

ERSTATNINGSANSVAR

1. Meldermedlemsstaten skal være ansvarlig for skader som forsettlig eller uaktsomt påføres en fysisk eller juridisk person på grunn av manglende overholdelse av forpliktelsene i henhold til artikkel 7 bokstav d) og f), i forbindelse med en transaksjon over landegrensene.
2. Parten som utsteder det elektroniske identifikasjonsmiddelet, skal være ansvarlig for skader som forsettlig eller uaktsomt påføres en fysisk eller juridisk person på grunn av manglende overholdelse av

forpliktelsen nevnt i artikkel 7 bokstav e), i forbindelse med en transaksjon over landegrensene.

3. Parten som utfører framgangsmåten for autentisering, skal være ansvarlig for skader som forsettlig eller uaktsomt påføres en fysisk eller juridisk person som følge av at autentiseringen nevnt i artikkel 7 bokstav f) ikke utføres på riktig måte, i forbindelse med en transaksjon over landegrensene.
4. Nr. 1, 2 og 3 får anvendelse i samsvar med nasjonale regler for erstatningsansvar.
5. Nr. 1, 2 og 3 berører ikke erstatningsansvaret som i henhold til nasjonal lovgivning påhviler parter i en transaksjon der det benyttes elektroniske identifikasjonsmidler som omfattes av ordningen for elektronisk identifikasjon meldt i henhold til artikkel 9 nr. 1.

ARTIKKEL 12

SAMARBEID OG SAMVIRKINGSEVNE

1. De nasjonale ordningene for elektronisk identifikasjon meldt i henhold til artikkel 9 nr. 1 skal være samvirkende.
2. Med hensyn til nr. 1 skal det opprettes en ramme for samvirkingsevne.
3. Rammen for samvirkingsevne skal oppfylle følgende kriterier:
   a) den har som mål å være teknologinøytral og skal ikke skille mellom spesifikke nasjonale tekniske løsninger for elektronisk identifikasjon i en medlemsstat,
   b) den følger europeiske og internasjonale standarder når det er mulig,
   c) den fremmer gjennomføringen av prinsippet om «innebygd personvern» og
   d) den sikrer at personopplysninger behandles i samsvar med direktiv 95/46/EF.
4. Rammen for samvirkingsevne skal bestå av
   a) en henvisning til tekniske minstekrav knyttet til sikkerhetsnivåene nevnt i artikkel 8,
   b) en sammenligningstabell over nasjonale sikkerhetsnivåer for meldte ordninger for elektronisk identifikasjon og sikkerhetsnivåene nevnt i artikkel 8,
   c) en henvisning til tekniske minstekrav til samvirkingsevne,
   d) en henvisning til et minstesett av personidentifikasjonsdata som på en entydig måte representerer en fysisk eller juridisk person, og som er tilgjengelig via ordninger for elektronisk identifikasjon,
   e) saksbehandlingsregler,
   f) tvisteløsningsordninger og
   g) felles standarder for driftssikkerhet.
5. Medlemsstatene skal samarbeide om følgende:
   a) samvirkingsevnen til ordningene for elektronisk identifikasjon meldt i henhold til artikkel 9 nr. 1 og ordningene for elektronisk identifikasjon som medlemsstatene har til hensikt å melde, og
   b) sikkerheten i ordningene for elektronisk identifikasjon.
6. Samarbeidet mellom medlemsstater skal bestå av
   a) utveksling av opplysninger, erfaring og god praksis med hensyn til ordninger for elektronisk identifikasjon og særlig tekniske krav knyttet til samvirkingsevne og sikkerhetsnivåer,
   b) utveksling av opplysninger, erfaring og god praksis med hensyn til bruk av sikkerhetsnivåene for ordninger for elektronisk identifikasjon nevnt i artikkel 8,
   c) fagfellevurdering av ordninger for elektronisk identifikasjon som omfattes av denne forordning, og
   d) undersøkelse av relevant utvikling i sektoren for elektronisk identifikasjon.
7. Innen 18. mars 2015 skal Kommisjonen ved hjelp av gjennomføringsrettsakter fastsette de nødvendige saksbehandlingsreglene for å forenkle samarbeidet mellom medlemsstatene nevnt i nr. 5 og 6 med henblikk på å fremme et høyt nivå av tillit og sikkerhet som står i forhold til graden av risiko.
8. Med henblikk på å fastsette ensartede vilkår for gjennomføringen av kravet i nr. 1, med forbehold for kriteriene fastsatt i nr. 3 og idet det tas hensyn til resultatene av samarbeidet mellom medlemsstatene, skal Kommisjonen innen 18. september 2015 vedta gjennomføringsrettsakter om rammen for samvirkingsevne som fastsatt i nr. 4.
9. Gjennomføringsrettsaktene nevnt i nr. 7 og 8 i denne artikkel skal vedtas etter framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

KAPITTEL III

TILLITSTJENESTER

AVSNITT 1

Alminnelige bestemmelser

ARTIKKEL 13

ERSTATNINGSANSVAR OG BEVISBYRDE

1. Med forbehold for nr. 2 skal tilbydere av tillitstjenester være ansvarlige for skader som forsettlig eller uaktsomt påføres en fysisk eller juridisk person på grunn av manglende overholdelse av forpliktelsene i denne forordning. Bevisbyrden for at en ikke-kvalifisert tilbyder av tillitstjenester har handlet forsettlig eller uaktsomt, påhviler den fysiske eller juri-

diske personen som hevder å ha lidd skadene nevnt i første ledd. En kvalifisert tilbyder av tillitstjenester formodes å ha handlet forsettlig eller uaktsomt, med mindre vedkommende beviser at skaden nevnt i første ledd oppsto uten at vedkommende har handlet forsettlig eller uaktsomt.

2. Når tilbydere av tillitstjenester på behørig vis underretter sine kunder på forhånd om begrensningene som gjelder for bruken av tjenestene de leverer, og når begrensningene er mulig å gjenkjenne for tredjeparter, skal tilbydere av tillitstjenester ikke være ansvarlige for skader som oppstår ved slik bruk av tjenester som overskrider de angitte begrensningene.
3. Nr. 1 og 2 får anvendelse i samsvar med nasjonale regler for erstatningsansvar.

ARTIKKEL 14

INTERNASJONALE ASPEKTER

1. Tillitstjenester som leveres av tilbydere av tillitstjenester etablert i en tredjestat, skal anerkjennes som rettslig likeverdige med kvalifiserte tillitstjenester som leveres av kvalifiserte tilbydere av tillitstjenester etablert i Unionen, dersom tillitstjenestene fra tredjestaten er anerkjent i henhold til en avtale inngått mellom Unionen og den berørte tredjestaten eller en internasjonal organisasjon i samsvar med artikkel 218 i TEUV.
2. Avtalene nevnt i nr. 1 skal særlig sikre at
   a) kravene som gjelder for kvalifiserte tilbydere av tillitstjenester etablert i Unionen og de kvalifiserte tillitstjenestene de leverer, oppfylles av tilbyderne av tillitstjenester i tredjestaten eller de internasjonale organisasjonene det er inngått avtale med, og av tillitstjenestene de leverer,
   b) de kvalifiserte tillitstjenestene som leveres av kvalifiserte tilbydere av tillitstjenester i Unionen, anerkjennes som rettslig likeverdige med tillitstjenester som leveres av tilbydere av tillitstjenester i tredjestaten eller den internasjonale organisasjonen som avtalen er inngått med.

ARTIKKEL 15

TILGJENGELIGHET FOR PERSONER MED NEDSATT FUNKSJONSEVNE

Når det er mulig, skal tillitstjenester og sluttbrukerprodukter som benyttes ved levering av slike tjenester, gjøres tilgjengelige for personer med nedsatt funksjonsevne.

ARTIKKEL 16

SANKSJONER

Medlemsstatene skal fastsette regler for sanksjoner som får anvendelse ved overtredelse av denne forordning. De fastsatte sanksjonene skal være virkningsfulle, stå i forhold til overtredelsen og virke avskrekkende.

AVSNITT 2

Tilsyn

ARTIKKEL 17

TILSYNSORGAN

1. Medlemsstatene skal utpeke et tilsynsorgan som er etablert på deres territorium eller, etter gjensidig avtale med en annen medlemsstat, et tilsynsorgan som er etablert i den andre medlemsstaten. Organet skal ha ansvar for tilsynsoppgaver i den utpekende medlemsstaten.

Tilsynsorganet skal gis nødvendig myndighet og tilstrekkelige ressurser til å kunne utføre sine oppgaver.

2. Medlemsstatene skal underrette Kommisjonen om navnene på og adressene til de utpekte tilsynsorganene.
3. Tilsynsorganet skal ha følgende rolle:
   a) føre tilsyn med kvalifiserte tilbydere av tillitstjenester som er etablert på den utpekende medlemsstatens territorium, for å sikre, gjennom tilsyn på forhånd og i ettertid, at de kvalifiserte tilbydere av tillitstjenester og de kvalifiserte tillitstjenestene de leverer, oppfyller kravene fastsatt i denne forordning,
   b) om nødvendig treffe tiltak overfor ikke-kvalifiserte tilbydere av tillitstjenester som er etablert på den utpekende medlemsstatens territorium, som følge av tilsyn i ettertid når det er blitt underrettet om at de ikke-kvalifiserte tilbyderne av tillitstjenester eller tillitstjenestene de leverer, angivelig ikke oppfyller kravene fastsatt i denne forordning.
4. Med hensyn til nr. 3 og med forbehold for begrensningene fastsatt i nevnte nummer skal tilsynsorganets oppgaver særlig omfatte å
   a) samarbeide med andre tilsynsorganer og bistå dem i samsvar med artikkel 18,
   b) analysere samsvarsvurderingsrapportene nevnt i artikkel 20 nr. 1 og 21 nr. 1,
   c) underrette andre tilsynsorganer og offentligheten om sikkerhetsbrudd eller tap av integritet i samsvar med artikkel 19 nr. 2,

d) framlegge rapport for Kommisjonen om sin hovedvirksomhet i samsvar med nr. 6 i denne artikkel,
e) foreta revisjoner eller anmode et samsvarsvurderingsorgan om å foreta en samsvarsvurdering av de kvalifiserte tilbyderne av tillitstjenester i samsvar med artikkel 20 nr. 2,
f) samarbeide med personvernmyndighetene, særlig ved å underrette dem så snart som mulig om resultatene fra revisjoner av kvalifiserte tilbydere av tillitstjenester, ved mistanke om at reglene for vern av personopplysninger ikke er overholdt,
g) tildele status som kvalifisert til tilbydere av tillitstjenester og tjenestene de leverer, og trekke tilbake denne statusen i samsvar med artikkel 20 og 21,
h) underrette organet med ansvar for den nasjonale tillitslisten nevnt i artikkel 22 nr. 3 om sine beslutninger om å tildele eller trekke tilbake status som kvalifisert, med mindre dette organet også er tilsynsorganet,
i) kontrollere at det foreligger bestemmelser om planer for opphør av virksomhet, og at de anvendes på riktig måte, i de tilfeller der kvalifiserte tilbydere av tillitstjenester innstiller sin virksomhet, herunder hvordan opplysninger forblir tilgjengelige i samsvar med artikkel 24 nr. 2 bokstav h),
j) kreve at tilbydere av tillitstjenester korrigerer enhver manglende overholdelse av kravene fastsatt i denne forordning.

5. Medlemsstatene kan kreve at tilsynsorganet oppretter, opprettholder og oppdaterer en tillitsinfrastruktur i samsvar med vilkårene i nasjonal lovgivning.
6. Innen 31. mars hvert år skal hvert tilsynsorgan framlegge en rapport for Kommisjonen om sin hovedvirksomhet i forrige kalenderår sammen med et sammendrag av meldingene om sikkerhetsbrudd som er mottatt fra tilbydere av tillitstjenester i samsvar med artikkel 19 nr. 2.
7. Kommisjonen skal gjøre den årlige rapporten nevnt i nr. 6 tilgjengelig for medlemsstatene.
8. Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette formatene og framgangsmåtene for rapporten nevnt i nr. 6. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

ARTIKKEL 18

GJENSIDIG BISTAND

1. Tilsynsorganene skal samarbeide om å utveksle god praksis.

Et tilsynsorgan skal etter mottak av en begrunnet anmodning fra et annet tilsynsorgan yte bistand til dette organet, slik at tilsynsorganenes virksomhet kan utføres på en ensartet måte. Gjensidig bistand kan særlig omfatte anmodninger om opplysninger og tilsynstiltak, for eksempel anmodninger om å foreta inspeksjoner knyttet til samsvarsvurderingsrapportene nevnt i artikkel 20 og 21.

2. Et tilsynsorgan som mottar en anmodning om bistand, kan avvise anmodningen med følgende begrunnelser:
   a) tilsynsorganet er ikke kompetent til å yte bistanden det anmodes om,
   b) bistanden det anmodes om, står ikke i forhold til tilsynsorganets tilsynsvirksomhet utført i samsvar med artikkel 17,
   c) det vil være uforenlig med denne forordning å yte bistanden det anmodes om.
3 Når det er relevant, kan medlemsstater tillate at deres respektive tilsynsorganer utfører felles undersøkelser der personale fra andre medlemsstaters tilsynsorganer deltar. Vilkårene og framgangsmåtene for slike felles tiltak skal avtales og fastsettes av de berørte medlemsstatene i samsvar med deres nasjonale lovgivning.

ARTIKKEL 19

SIKKERHETSKRAV SOM GJELDER FOR TILBYDERE AV TILLITSTJENESTER

1. Kvalifiserte og ikke-kvalifiserte tilbydere av tillitstjenester skal treffe egnede tekniske og organisatoriske tiltak for å håndtere sikkerhetsrisikoer i forbindelse med tillitstjenestene de leverer. Idet det tas hensyn til den siste teknologiske utviklingen, skal nevnte tiltak sikre at sikkerhetsnivået står i forhold til graden av risiko. Det skal særlig treffes tiltak for å forebygge og minimere virkningen av sikkerhetshendelser samt for å underrette berørte parter om skadevirkningene av slike hendelser.
2. Kvalifiserte og ikke-kvalifiserte tilbydere av tillitstjenester skal så snart som mulig og senest 24 timer etter å ha fått kjennskap til sikkerhetsbrudd eller tap av integritet som i betydelig grad påvirker tillitstjenesten eller personopplysninger som oppbevares i forbindelse med levering av tjenesten, underrette tilsynsorganet og eventuelt andre berørte

organer, for eksempel vedkommende nasjonale organ for informasjonssikkerhet eller personvernmyndighet.

Dersom det er trolig at et sikkerhetsbrudd eller tap av integritet vil ha negativ innvirkning på en fysisk eller juridisk person som har benyttet seg av tillitstjenesten, skal tilbyderen av tillitstjenesten så snart som mulig også underrette den fysiske eller juridiske personen om sikkerhetsbruddet eller tapet av integritet.

Når det er relevant, særlig dersom et sikkerhetsbrudd eller tap av integritet gjelder to eller flere medlemsstater, skal det meldte tilsynsorganet underrette tilsynsorganene i andre berørte medlemsstater samt ENISA.

Det meldte tilsynsorganet skal underrette offentligheten eller kreve at tilbyderen av tillitstjenestene gjør dette, dersom det fastslår at det er i offentlighetens interesse at sikkerhetsbruddet eller tapet av integritet offentliggjøres.

3. Tilsynsorganet skal én gang i året framlegge for ENISA et sammendrag av meldingene om sikkerhetsbrudd og tap av integritet som er mottatt fra tilbydere av tillitstjenester.
4. Kommisjonen kan ved hjelp av gjennomføringsrettsakter
   a) spesifisere tiltakene nevnt i nr. 1 ytterligere og
   b) fastsette formater og framgangsmåter, herunder tidsfrister, som gjelder for nr. 2.

Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

AVSNITT 3

Kvalifiserte tillitstjenester

ARTIKKEL 20

TILSYN MED KVALIFISERTE TILBYDERE AV TILLITSTJENESTER

1. Kvalifiserte tilbydere av tillitstjenester skal minst hver 24. måned og for egen regning revideres av et samsvarsvurderingsorgan. Formålet med revisjonen er å bekrefte at de kvalifiserte tilbyderne av tillitstjenester og de kvalifiserte tillitstjenestene de leverer, oppfyller kravene fastsatt i denne forordning. De kvalifiserte tilbyderne av tillitstjenester skal framlegge samsvarsvurderingsrapporten for tilsynsorganet innen tre virkedager etter at den er mottatt.
2. Med forbehold for nr. 1 kan tilsynsorganet til enhver tid foreta revisjon eller anmode et samsvarsvurderingsorgan om å foreta en samsvarsvurdering av de kvalifiserte tilbyderne av tillitstjenester, for tilbyderne av tillitstjenester sin regning, for å bekrefte at de og de kvalifiserte tillitstjenestene de leverer, oppfyller kravene fastsatt i denne forordning. Ved mistanke om at reglene for vern av personopplysninger ikke er overholdt, skal tilsynsorganet underrette personvernmyndighetene om resultatene av sine revisjoner.
3. Dersom tilsynsorganet krever at den kvalifiserte tilbyderen av tillitstjenester skal korrigere en eventuell manglende overholdelse av kravene fastsatt i denne forordning, og dersom tjenestetilbyderen ikke retter seg etter dette, eventuelt innen en tidsfrist fastsatt av tilsynsorganet, kan tilsynsorganet, idet det særlig tar hensyn til omfanget, varigheten og følgene av den manglende overholdelsen, trekke tilbake status som kvalifisert for tjenestetilbyderen eller tjenesten denne leverer, og underrette organet nevnt i artikkel 22 nr. 3 for å få ajourført tillitslistene nevnt i artikkel 22 nr. 1. Tilsynsorganet skal underrette den kvalifiserte tilbyderen av tillitstjenester om tilbaketrekkingen av vedkommendes eller den berørte tjenestens status som kvalifisert.
4. Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenumre for følgende standarder:
   a) akkreditering av samsvarsvurderingsorganer og for samsvarsvurderingsrapporten nevnt i nr. 1,
   b) revisjonsregler som samsvarsvurderingsorganer skal følge ved samsvarsvurdering av de kvalifiserte tilbyderne av tillitstjenester nevnt i nr. 1.

Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

ARTIKKEL 21

LANSERING AV EN KVALIFISERT TILLITSTJENESTE

1. Dersom tilbydere av tillitstjenester som ikke har status som kvalifisert, har til hensikt å begynne å levere kvalifiserte tillitstjenester, skal de underrette tilsynsorganet om dette og samtidig framlegge en samsvarsvurderingsrapport utstedt av et samsvarsvurderingsorgan.
2. Tilsynsorganet skal kontrollere om tilbyderen av tillitstjenester og tillitstjenestene denne leverer, oppfyller kravene fastsatt i denne forordning, og særlig kravene til kvalifiserte tilbydere av tillitstjenester og til de kvalifiserte tillitstjenestene de leverer.

Dersom tilsynsorganet fastslår at tilbyderen av tillitstjenester og tillitstjenestene denne leverer, oppfyller kravene nevnt i første ledd, skal tilsynsorganet gi status

som kvalifisert til tilbyderen av tillitstjenester og tillitstjenestene denne leverer, og underrette organet nevnt i artikkel 22 nr. 3 for å få ajourført tillitslistene nevnt i artikkel 22 nr. 1 senest tre måneder etter underretningen i samsvar med nr. 1 i denne artikkel.

Dersom kontrollen ikke er avsluttet innen tre måneder etter underretningen, skal tilsynsorganet underrette tilbyderen av tillitstjenester om dette og angi årsakene til forsinkelsen og tidspunktet for når kontrollen skal være avsluttet.

3. Kvalifiserte tilbydere av tillitstjenester kan begynne å levere den kvalifiserte tillitstjenesten når status som kvalifisert er angitt i tillitslistene nevnt i artikkel 22 nr. 1.
4. Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette formater og framgangsmåter som gjelder for nr. 1 og 2. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

ARTIKKEL 22

TILLITSLISTER

1. Hver medlemsstat skal opprette, ajourføre og offentliggjøre tillitslister med opplysninger om de kvalifiserte tilbyderne av tillitstjenester som den har ansvar for, sammen med opplysninger om de kvalifiserte tillitstjenestene de leverer.
2. Medlemsstatene skal på en sikker måte opprette, ajourføre og offentliggjøre de elektronisk signerte eller forseglede tillitslistene nevnt i nr. 1 i en form som er egnet for automatisert behandling.
3. Medlemsstatene skal så snart som mulig underrette Kommisjonen om hvilket organ som er ansvarlig for å opprette, ajourføre og offentliggjøre nasjonale tillitslister, og om hvor slike lister offentliggjøres, om sertifikatene som brukes til å signere eller forsegle tillitslistene, og om eventuelle endringer av dette.
4. Kommisjonen skal gjøre opplysningene nevnt i nr. 3 offentlig tilgjengelige via en sikker kanal i elektronisk signert eller forseglet form egnet for automatisert behandling.
5. Innen 18. september 2015 skal Kommisjonen ved hjelp av gjennomføringsrettsakter presisere opplysningene nevnt i nr. 1 og fastsette tekniske spesifikasjoner og formater som skal gjelde for tillitslister med hensyn til nr. 1–4. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

ARTIKKEL 23

EU-TILLITSMERKE FOR KVALIFISERTE TILLITSTJENESTER

1. Når status som kvalifisert nevnt i artikkel 21 nr. 2 annet ledd er angitt i tillitslisten nevnt i artikkel 22 nr. 1, kan kvalifiserte tilbydere av tillitstjenester bruke EU-tillitsmerket for på en enkel, gjenkjennelig og tydelig måte angi de kvalifiserte tillitstjenestene de leverer.
2. Ved bruk av EU-tillitsmerket for de kvalifiserte tillitstjenestene nevnt i nr. 1 skal kvalifiserte tilbydere av tillitstjenester sørge for at deres nettsted inneholder en lenke til den relevante tillitslisten.
3. Innen 1. juli 2015 skal Kommisjonen ved hjelp av gjennomføringsrettsakter fastsette spesifikasjoner med hensyn til formen og særlig presentasjonen, sammensetningen, størrelsen og utformingen av EU-tillitsmerket for kvalifiserte tillitstjenester. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

ARTIKKEL 24

KRAV TIL KVALIFISERTE TILBYDERE AV TILLITSTJENESTER

1. Når en kvalifisert tilbyder av tillitstjenester utsteder et kvalifisert sertifikat for en tillitstjeneste, skal vedkommende ved hjelp av egnede midler og i samsvar med nasjonal lovgivning kontrollere identiteten til og, dersom det er relevant, eventuelle særlige egenskaper ved den fysiske eller juridiske personen som det kvalifiserte sertifikatet utstedes til.

Opplysningene nevnt i første ledd skal kontrolleres av den kvalifiserte tilbyderen av tillitstjenester enten direkte eller via en tredjepart i samsvar med nasjonal lovgivning:

a) ved fysisk tilstedeværelse av den fysiske personen eller en godkjent representant for den juridiske personen eller
b) uten fysisk tilstedeværelse ved bruk av elektroniske identifikasjonsmidler, der det før utstedelsen av det kvalifiserte sertifikatet var sikret fysisk tilstedeværelse av den fysiske personen eller en godkjent representant for den juridiske personen, og som oppfyller kravene fastsatt i artikkel 8 med hensyn til sikkerhetsnivåene «betydelig» eller «høyt», eller
c) ved hjelp av et sertifikat for en kvalifisert elektronisk signatur eller et kvalifisert elektronisk segl utstedt i samsvar med bokstav a) eller b) eller
d) ved bruk av andre identifikasjonsmetoder anerkjent på nasjonalt plan som garanterer pålitelighet som tilsvarer fysisk tilstedeværelse. Et samsvarsvur-

deringsorgan skal bekrefte at garantiene er likeverdige.

2. En kvalifisert tilbyder av tillitstjenester som tilbyr kvalifiserte tillitstjenester, skal
   a) underrette tilsynsorganet om eventuelle endringer i leveringen av sine kvalifiserte tillitstjenester og om en eventuell hensikt om å innstille denne virksomheten,
   b) ha personale og eventuelt underleverandører med den nødvendige sakkunnskap, pålitelighet, erfaring og kvalifikasjoner som har fått egnet opplæring med hensyn til sikkerhet og regler for vern av personopplysninger, og skal anvende administrative og forvaltningsmessige framgangsmåter som er i samsvar med europeiske eller internasjonale standarder,
   c) når det gjelder risikoen for erstatningsansvar i samsvar med artikkel 13, ha tilstrekkelige økonomiske midler og/eller tegne en egnet ansvarsforsikring i samsvar med nasjonal lovgivning,
   d) før inngåelse av et kontraktsforhold, på en tydelig og forståelig måte opplyse enhver person som ønsker å benytte en kvalifisert tillitstjeneste, om de nøyaktige vilkårene for bruk av denne tjenesten, herunder eventuelle bruksbegrensninger,
   e) benytte pålitelige systemer og produkter som er beskyttet mot endringer, og sikre den tekniske sikkerheten og påliteligheten i de prosessene som støttes av disse,
   f) benytte pålitelige systemer til lagring av dataene den mottar, i en kontrollerbar form slik at
      i) de er offentlig tilgjengelige bare dersom det er innhentet samtykke fra personen som dataene gjelder,
      ii) bare autoriserte personer kan legge inn opplysninger og gjøre endringer i de lagrede dataene,
      iii)dataenes ekthet kan kontrolleres,
   g) treffe egnede tiltak mot forfalskning og tyveri av data,
   h) registrere alle relevante opplysninger om data som den kvalifiserte tilbyderen av tillitstjenester har utstedt og mottatt, og sørge for at de er tilgjengelige i et rimelig tidsrom, herunder etter at virksomheten til den kvalifiserte tilbyderen av tillitstjenester er innstilt, særlig for å kunne framlegge bevis i forbindelse med rettergang og å sikre kontinuitet i tjenesten. Slik registrering kan gjøres elektronisk,
   i) ha en ajourført plan for opphør av virksomhet for å sikre kontinuitet i tjenesten i samsvar med bestemmelsene kontrollert av tilsynsorganet i samsvar med artikkel 17 nr. 4 bokstav i),
   j) sikre rettmessig behandling av personopplysninger i samsvar med direktiv 95/46/EF,
   k) dersom kvalifiserte tilbydere av tillitstjenester utsteder sertifikater, opprette og holde oppdatert en sertifikatdatabase.
3. Dersom en kvalifisert tilbyder av tillitstjenester som utsteder kvalifiserte sertifikater, beslutter å tilbakekalle et sertifikat, skal den registrere tilbakekallingen i sin sertifikatdatabase og offentliggjøre sertifikatets status som tilbakekalt i god tid, og i alle tilfeller innen 24 timer etter mottak av anmodningen. Tilbakekallingen skal tre i kraft umiddelbart etter at den er offentliggjort.
4. Med hensyn til nr. 3 skal kvalifiserte tilbydere av tillitstjenester som utsteder kvalifiserte sertifikater, informere eventuelle tjenestebrukere om gyldigheten av eller status som tilbakekalt for kvalifiserte sertifikater som er utstedt av dem. Slike opplysninger skal minst gjøres tilgjengelige for hvert enkelt sertifikat, når som helst og utover sertifikatets gyldighetsperiode på en automatisert måte som er pålitelig, gratis og effektiv.
5. Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenumre for standarder for pålitelige systemer og produkter som oppfyller kravene i nr. 2 bokstav e) og f) i denne artikkel. Dersom pålitelige systemer og produkter oppfyller kravene i nevnte standarder, skal de formodes å oppfylle kravene i denne artikkel. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

AVSNITT 4

Elektroniske signaturer

ARTIKKEL 25

RETTSVIRKNINGER AV ELEKTRONISKE SIGNATURER

1. En elektronisk signatur skal ikke nektes rettsvirkning og gyldighet som bevis i forbindelse med rettergang alene av den grunn at den er elektronisk, eller at den ikke oppfyller kravene til kvalifiserte elektroniske signaturer.
2. En kvalifisert elektronisk signatur skal ha samme rettsvirkning som en håndskreven signatur.
3. En kvalifisert elektronisk signatur som er basert på et kvalifisert sertifikat utstedt i én medlemsstat, skal anerkjennes som en kvalifisert elektronisk signatur i alle andre medlemsstater.

ARTIKKEL 26

KRAV TIL AVANSERTE ELEKTRONISKE SIGNATURER

En avansert elektronisk signatur skal oppfylle følgende krav:

a) den er entydig knyttet til underskriveren,
b) den kan identifisere underskriveren,
c) den er framstilt ved hjelp av elektroniske signaturframstillingsdata som underskriveren, med en høy grad av pålitelighet, har enekontroll over bruken av, og
d) den er knyttet til dataene som er signert med denne signaturen, på en slik måte at eventuelle etterfølgende endringer i dataene kan oppdages.

ARTIKKEL 27

ELEKTRONISKE SIGNATURER I OFFENTLIGE TJENESTER

1. Dersom en medlemsstat krever en avansert elektronisk signatur for å bruke en nettbasert tjeneste som tilbys av eller på vegne av et offentlig organ, skal medlemsstaten anerkjenne avanserte elektroniske signaturer, avanserte elektroniske signaturer basert på et kvalifisert sertifikat for elektroniske signaturer og kvalifiserte elektroniske signaturer i minst de formatene eller ved bruk av metodene som er fastsatt i gjennomføringsrettsaktene nevnt i nr. 5.
2. Dersom en medlemsstat krever en avansert elektronisk signatur basert på et kvalifisert sertifikat for å bruke en nettbasert tjeneste som tilbys av eller på vegne av et offentlig organ, skal medlemsstaten anerkjenne avanserte elektroniske signaturer basert på et kvalifisert sertifikat og kvalifiserte elektroniske signaturer i minst de formatene eller ved bruk av metodene som er fastsatt i gjennomføringsrettsaktene nevnt i nr. 5.
3. Ved bruk over landegrensene i en nettbasert tjeneste som tilbys av et offentlig organ, skal medlemsstatene ikke kreve en elektronisk signatur med et høyere sikkerhetsnivå enn det som gjelder for den kvalifiserte elektroniske signaturen.
4. Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenumre for standarder for avanserte elektroniske signaturer. Dersom en avansert elektronisk signatur oppfyller kravene i nevnte standarder, skal den formodes å oppfylle kravene til avanserte elektroniske signaturer nevnt i nr. 1 og 2 i denne artikkel og i artikkel 26. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.
5. Innen 18. september 2015 og idet det tas hensyn til eksisterende praksis, standarder og EU-rettsakter skal Kommisjonen ved hjelp av gjennomføringsrettsakter fastsette referanseformater for avanserte elektroniske signaturer eller referansemetoder dersom alternative formater brukes. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

ARTIKKEL 28

KVALIFISERTE SERTIFIKATER FOR ELEKTRONISKE SIGNATURER

1. Kvalifiserte sertifikater for elektroniske signaturer skal oppfylle kravene fastsatt i vedlegg I.
2. Kvalifiserte sertifikater for elektroniske signaturer skal ikke omfattes av ufravikelige krav som går lenger enn kravene fastsatt i vedlegg I.
3. Kvalifiserte sertifikater for elektroniske signaturer kan omfatte ikke-obligatoriske særlige tilleggsattributter. Nevnte attributter skal ikke påvirke samvirkingsevnen til og anerkjennelsen av kvalifiserte elektroniske signaturer.
4. Dersom et kvalifisert sertifikat for elektroniske signaturer er blitt tilbakekalt etter første aktivering, skal det miste gyldighet fra tilbakekallingstidspunktet, og dets status skal ikke under noen omstendigheter gjenopprettes.
5. Medlemsstatene kan fastsette nasjonale regler for midlertidig oppheving av et kvalifisert sertifikat for elektronisk signatur på følgende vilkår:
   a) dersom et kvalifisert sertifikat for elektronisk signatur er blitt midlertidig opphevet, skal sertifikatet miste sin gyldighet i opphevingsperioden,
   b) opphevingsperioden skal angis tydelig i sertifikatdatabasen, og i opphevingsperioden skal statusen som midlertidig opphevet være synlig gjennom tjenesten som formidler opplysninger om sertifikatets status.
6. Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenumre for standarder for kvalifiserte sertifikater for elektronisk signaturer. Dersom et kvalifisert sertifikat for elektronisk signatur oppfyller kravene i nevnte standarder, skal det formodes å oppfylle kravene fastsatt i vedlegg I. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

ARTIKKEL 29

KRAV TIL KVALIFISERTE ELEKTRONISKE SIGNATURFRAMSTILLINGSSYSTEMER

1. Kvalifiserte elektroniske signaturframstillingssystemer skal oppfylle kravene fastsatt i vedlegg II.
2. Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenumre for standarder

for kvalifiserte elektroniske signaturframstillingssystemer. Dersom et kvalifisert elektronisk signaturframstillingssystem oppfyller kravene i nevnte standarder, skal det formodes å oppfylle kravene fastsatt i vedlegg II. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

ARTIKKEL 30

SERTIFISERING AV KVALIFISERTE ELEKTRONISKE SIGNATURFRAMSTILLINGSSYSTEMER

1. Egnede offentlige eller private organer utpekt av medlemsstatene skal sertifisere at kvalifiserte elektroniske signaturframstillingssystemer oppfyller kravene fastsatt i vedlegg II.
2. Medlemsstatene skal underrette Kommisjonen om navnet på og adressen til det offentlige eller private organet nevnt i nr. 1. Kommisjonen skal gjøre disse opplysningene tilgjengelige for medlemsstatene.
3. Sertifiseringen nevnt i nr. 1 skal bygge på ett av følgende elementer:
   a) en sikkerhetsvurderingsprosess utført i samsvar med en av standardene for sikkerhetsvurdering av informasjonsteknologiprodukter oppført på listen opprettet i samsvar med annet ledd, eller
   b) en annen prosess enn prosessen nevnt i bokstav a), forutsatt at den omfatter sammenlignbare sikkerhetsnivåer, og forutsatt at det offentlige eller private organet nevnt i nr. 1 melder prosessen til Kommisjonen. Denne prosessen kan brukes bare dersom standardene nevnt i bokstav a) ikke foreligger, eller dersom det pågår en sikkerhetsvurderingsprosess som nevnt i bokstav a).

Kommisjonen skal ved hjelp av gjennomføringsrettsakter opprette en liste over standarder med henblikk på sikkerhetsvurderingen av informasjonsteknologiprodukter nevnt i bokstav a). Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

4. Kommisjonen skal gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 47 om fastsettelse av spesifikke kriterier som skal oppfylles av de utpekte organene nevnt i nr. 1 i denne artikkel.

ARTIKKEL 31

OFFENTLIGGJØRING AV EN LISTE OVER SERTIFISERTE KVALIFISERTE ELEKTRONISKE SIGNATURFRAMSTILLINGSSYSTEMER

1. Medlemsstatene skal så raskt som mulig og senest én måned etter at sertifiseringen er avsluttet, framlegge for Kommisjonen opplysninger om de kvalifiserte systemene for framstilling av elektroniske signaturer som er blitt sertifisert av organene nevnt i artikkel 30 nr. 1. De skal også så raskt som mulig og senest én måned etter at sertifiseringen er annullert, framlegge for Kommisjonen opplysninger om de systemene for framstilling av elektroniske signaturer som ikke lenger er sertifisert.
2. På grunnlag av de mottatte opplysningene skal Kommisjonen opprette, offentliggjøre og ajourføre en liste over sertifiserte kvalifiserte elektroniske signaturframstillingssystemer.
3. Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette formater og framgangsmåter som gjelder for nr. 1. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

ARTIKKEL 32

KRAV TIL VALIDERING AV KVALIFISERTE ELEKTRONISKE SIGNATURER

1. Prosessen for validering av en kvalifisert elektronisk signatur skal bekrefte gyldigheten av en kvalifisert elektronisk signatur, forutsatt at
   a) sertifikatet som støtter signaturen, på signeringstidspunktet var et kvalifisert sertifikat for elektronisk signatur som oppfyller kravene i vedlegg I,
   b) det kvalifiserte sertifikatet er utstedt av en kvalifisert tilbyder av tillitstjenester og var gyldig på signeringstidspunktet,
   c) signaturvalideringsdataene stemmer overens med dataene som stilles til rådighet for tjenestebrukeren,
   d) det entydige datasettet som representerer underskriveren i sertifikatet, stilles til rådighet på riktig måte for tjenestebrukeren,
   e) bruken av et pseudonym framgår tydelig for tjenestebrukeren dersom det på signeringstidspunktet ble brukt et pseudonym,
   f) den elektroniske signaturen er framstilt av et kvalifisert elektronisk signaturframstillingssystem,
   g) integriteten til de signerte dataene er intakt,
   h) kravene fastsatt i artikkel 26 er oppfylt på signeringstidspunktet.
2. Systemet som brukes for å validere den kvalifiserte elektroniske signaturen, skal gi tjenestebrukeren det riktige resultatet av valideringsprosessen og gjøre det mulig for tjenestebrukeren å oppdage eventuelle problemer knyttet til sikkerheten.
3. Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenumre for standarder for validering av kvalifiserte elektroniske signaturer. Dersom valideringen av kvalifiserte elektro-

niske signaturer oppfyller kravene i nevnte standarder, skal den formodes å oppfylle kravene fastsatt i nr. 1. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

ARTIKKEL 33

KVALIFISERT VALIDERINGSTJENESTE FOR KVALIFISERTE ELEKTRONISKE SIGNATURER

1. En kvalifisert valideringstjeneste for kvalifiserte elektroniske signaturer kan leveres bare av en kvalifisert tilbyder av tillitstjenester som
   a) tilbyr validering i samsvar med artikkel 32 nr. 1, og
   b) lar tjenestebrukere motta resultatet av valideringsprosessen på en automatisert måte som er pålitelig og effektiv, påført den avanserte elektroniske signaturen eller det avanserte elektroniske seglet til tilbyderen av den kvalifiserte valideringstjenesten.
2. Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenumre for standarder for kvalifiserte valideringstjenester nevnt i nr. 1. Dersom valideringstjenesten for en kvalifisert elektronisk signatur oppfyller kravene i nevnte standarder, skal den formodes å oppfylle kravene fastsatt i nr. 1. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

ARTIKKEL 34

KVALIFISERT TJENESTE FOR BEVARING AV KVALIFISERTE ELEKTRONISKE SIGNATURER

1. En kvalifisert tjeneste for bevaring av kvalifiserte elektroniske signaturer kan leveres bare av en kvalifisert tilbyder av tillitstjenester som benytter framgangsmåter og teknologi som gjør det mulig å forlenge påliteligheten til den kvalifiserte elektroniske signaturen utover den teknologiske gyldighetstiden.
2. Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenumre for standarder for den kvalifiserte tjenesten for bevaring av kvalifiserte elektroniske signaturer. Dersom den kvalifiserte tjenesten for bevaring av elektroniske signaturer oppfyller kravene i nevnte standarder, skal den formodes å oppfylle kravene fastsatt i nr. 1. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

AVSNITT 5

Elektroniske segl

ARTIKKEL 35

RETTSVIRKNINGER AV ELEKTRONISKE SEGL

1. Et elektronisk segl skal ikke nektes rettsvirkning og gyldighet som bevis i forbindelse med rettergang alene av den grunn at det er elektronisk, eller at det ikke oppfyller kravene til kvalifiserte elektroniske segl.
2. For et kvalifisert elektronisk segl skal det formodes at integriteten til dataene som det kvalifiserte elektroniske seglet er knyttet til, er intakt, og at dataenes opprinnelse er riktig.
3. Et kvalifisert elektronisk segl som er basert på et kvalifisert sertifikat utstedt i én medlemsstat, skal anerkjennes som et kvalifisert elektronisk segl i alle andre medlemsstater.

ARTIKKEL 36

KRAV TIL AVANSERTE ELEKTRONISKE SEGL

Et avansert elektronisk segl skal oppfylle følgende krav:

a) det er entydig knyttet til seglframstilleren,
b) det kan identifisere seglframstilleren,
c) det er framstilt ved hjelp av elektroniske seglframstillingsdata som seglframstilleren, med en høy grad av pålitelighet, har under sin kontroll og kan bruke til framstilling av elektroniske segl, og
d) det er knyttet til dataene det gjelder, på en slik måte at eventuelle etterfølgende endringer i dataene kan oppdages.

ARTIKKEL 37

ELEKTRONISKE SEGL I OFFENTLIGE TJENESTER

1. Dersom en medlemsstat krever et avansert elektronisk segl for å bruke en nettbasert tjeneste som tilbys av eller på vegne av et offentlig organ, skal medlemsstaten anerkjenne avanserte elektroniske segl, avanserte elektroniske segl basert på et kvalifisert sertifikat for elektroniske segl og kvalifiserte elektroniske segl i minst de formatene eller ved bruk av metodene som er fastsatt i gjennomføringsrettsaktene nevnt i nr. 5.
2. Dersom en medlemsstat krever et avansert elektronisk segl basert på et kvalifisert sertifikat for å bruke en nettbasert tjeneste som tilbys av eller på vegne av et offentlig organ, skal medlemsstaten anerkjenne avanserte elektroniske segl basert på et kvalifisert sertifikat og kvalifiserte elektroniske segl i minst de

formatene eller ved bruk av metodene som er fastsatt i gjennomføringsrettsaktene nevnt i nr. 5.

3. Ved bruk over landegrensene i en nettbasert tjeneste som tilbys av et offentlig organ, skal medlemsstatene ikke kreve et elektronisk segl med et høyere sikkerhetsnivå enn det som gjelder for det kvalifiserte elektroniske seglet.
4. Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenumre for standarder for avanserte elektroniske segl. Dersom et avansert elektronisk segl oppfyller kravene i nevnte standarder, skal det formodes å oppfylle kravene til avanserte elektroniske segl nevnt i nr. 1 og 2 i denne artikkel og i artikkel 36. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.
5. Innen 18. september 2015 og idet det tas hensyn til eksisterende praksis, standarder og EU-rettsakter skal Kommisjonen ved hjelp av gjennomføringsrettsakter fastsette referanseformater for avanserte elektroniske segl eller referansemetoder dersom alternative formater brukes. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

ARTIKKEL 38

KVALIFISERTE SERTIFIKATER FOR ELEKTRONISKE SEGL

1. Kvalifiserte sertifikater for elektroniske segl skal oppfylle kravene fastsatt i vedlegg III.
2. Kvalifiserte sertifikater for elektroniske segl skal ikke omfattes av ufravikelige krav som går lenger enn kravene fastsatt i vedlegg III.
3. Kvalifiserte sertifikater for elektroniske segl kan omfatte ikke-obligatoriske særlige tilleggsattributter. Nevnte attributter skal ikke påvirke samvirkingsevnen til og anerkjennelsen av kvalifiserte elektroniske segl.
4. Dersom et kvalifisert sertifikat for et elektronisk segl er blitt tilbakekalt etter første aktivering, skal det miste sin gyldighet fra tilbakekallingstidspunktet, og dets status skal ikke under noen omstendigheter gjenopprettes.
5. Medlemsstatene kan fastsette nasjonale regler for midlertidig oppheving av kvalifiserte sertifikater for elektroniske segl på følgende vilkår:
   a) dersom et kvalifisert sertifikat for et elektroniske segl er blitt midlertidig opphevet, skal sertifikatet miste sin gyldighet i opphevingsperioden,
   b) opphevingsperioden skal angis tydelig i sertifikatdatabasen, og i opphevingsperioden skal statusen som midlertidig opphevet være synlig gjennom tjenesten som formidler opplysninger om sertifikatets status.
6. Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenumre for standarder for kvalifiserte sertifikater for elektroniske segl. Dersom et kvalifisert sertifikat for elektroniske segl oppfyller kravene i nevnte standarder, skal det formodes å oppfylle kravene fastsatt i vedlegg III. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

ARTIKKEL 39

KVALIFISERTE ELEKTRONISKE SEGLFRAMSTILLINGSSYSTEMER

1. Artikkel 29 får tilsvarende anvendelse på krav til kvalifiserte elektroniske seglframstillingssystemer.
2. Artikkel 30 får tilsvarende anvendelse på sertifisering av kvalifiserte elektroniske seglframstillingssystemer.
3. Artikkel 31 får tilsvarende anvendelse på offentliggjøring av en liste over sertifiserte kvalifiserte elektroniske seglframstillingssystemer.

ARTIKKEL 40

VALIDERING OG BEVARING AV KVALIFISERTE ELEKTRONISKE SEGL

Artikkel 32, 33 og 34 får tilsvarende anvendelse på validering og bevaring av kvalifiserte elektroniske segl.

AVSNITT 6

Elektroniske tidsstempler

ARTIKKEL 41

RETTSVIRKNING AV ELEKTRONISKE TIDSSTEMPLER

1. Et elektronisk tidsstempel skal ikke nektes rettsvirkning og gyldighet som bevis i forbindelse med rettergang alene av den grunn at det er elektronisk, eller at det ikke oppfyller kravene til et kvalifisert elektronisk tidsstempel.
2. For et kvalifisert elektronisk tidsstempel skal det formodes at datoen og tidspunktet det angir, er nøyaktig, og at integriteten til dataene som datoen og tidspunktet er knyttet til, er intakt.
3. Et kvalifisert elektronisk tidsstempel utstedt i én medlemsstat skal anerkjennes som et kvalifisert elektronisk tidsstempel i alle andre medlemsstater.

ARTIKKEL 42

KRAV TIL KVALIFISERTE ELEKTRONISKE TIDSSTEMPLER

1. Et kvalifisert elektronisk tidsstempel skal oppfylle følgende krav:
   a) det knytter datoen og tidspunktet til dataene på en slik måte at muligheten for at dataene endres uten at det oppdages, med rimelighet kan utelukkes,
   b)det bygger på en nøyaktig tidskilde som er knyttet til koordinert universell tid, og
   c) det er signert ved bruk av en avansert elektronisk signatur eller forseglet med et avansert elektronisk segl tilhørende den kvalifiserte tilbyderen av tillitstjenester, eller med en annen tilsvarende metode.
2. Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenumre for standarder for å knytte dato og tidspunkt til data og for nøyaktige tidskilder. Dersom tilknytningen mellom dato/tidspunkt og data samt den nøyaktige tidskilden oppfyller kravene i nevnte standarder, skal den formodes å oppfylle kravene fastsatt i nr. 1. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

AVSNITT 7

Elektroniske tjenester for registrert sending

ARTIKKEL 43

RETTSVIRKNING AV EN ELEKTRONISK TJENESTE FOR REGISTRERT SENDING

1. Data som sendes og mottas ved hjelp av en elektronisk tjeneste for registrert sending, skal ikke nektes rettsvirkning og gyldighet som bevis i forbindelse med rettergang alene av den grunn at de er elektroniske, eller at de ikke oppfyller kravene til den kvalifiserte elektroniske tjenesten for registrert sending.
2. Data som sendes og mottas ved hjelp av en kvalifisert elektronisk tjeneste for registrert sending, skal omfattes av en formodning om dataenes integritet, den identifiserte senderens sending av dataene, den identifiserte mottakerens mottak av dataene og nøyaktigheten av datoen og tidspunktet for sending og mottak som angis av den kvalifiserte elektroniske tjenesten for registrert sending.

ARTIKKEL 44

KRAV TIL KVALIFISERTE ELEKTRONISKE TJENESTER FOR REGISTRERT SENDING

1. Kvalifiserte elektroniske tjenester for registrert sending skal oppfylle følgende krav:
   a) de leveres av én eller flere kvalifiserte tilbydere av tillitstjenester,
   b) de sikrer identifikasjon av senderen med en høy grad av pålitelighet,
   c) de sikrer identifikasjon av mottakeren før dataene leveres,
   d) sending og mottak av data sikres ved hjelp av en avansert elektronisk signatur eller et avansert elektronisk segl tilhørende en kvalifisert tilbyder av tillitstjenester på en slik måte at det utelukker muligheten for at dataene endres uten at det oppdages,
   e) enhver endring av dataene som er nødvendig for å sende eller motta dataene, angis tydelig for senderen og mottakeren av dataene,
   f) datoen og tidspunktet for sending, mottak og eventuelle endringer av dataene angis ved hjelp av et kvalifisert elektronisk tidsstempel.

   Dersom dataene overføres mellom to eller flere kvalifiserte tilbydere av tillitstjenester, får kravene i bokstav a)–f) anvendelse på alle de kvalifiserte tilbyderne av tillitstjenester.
2. Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenumre for standarder for prosesser for sending og mottak av data. Dersom prosessen for sending og mottak av data oppfyller kravene i nevnte standarder, skal den formodes å oppfylle kravene fastsatt i nr. 1. Disse gjennomføringsrettsaktene skal vedtas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

AVSNITT 8

Nettstedsautentisering

ARTIKKEL 45

KRAV TIL KVALIFISERTE SERTIFIKATER FOR NETTSTEDSAUTENTISERING

1. Kvalifiserte sertifikater for nettstedsautentisering skal oppfylle kravene fastsatt i vedlegg IV.
2. Kommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenumre for standarder for kvalifiserte sertifikater for nettstedsautentisering. Dersom et kvalifisert sertifikat for nettstedsautentisering oppfyller kravene i nevnte standarder, skal det formodes å oppfylle kravene fastsatt i vedlegg IV. Disse gjennomføringsrettsaktene skal ved-

tas i samsvar med framgangsmåten med undersøkelseskomité nevnt i artikkel 48 nr. 2.

KAPITTEL IV

ELEKTRONISKE DOKUMENTER

Artikkel 46

Rettsvirkninger av elektroniske dokumenter

Et elektronisk dokument skal ikke nektes rettsvirkning og gyldighet som bevis i forbindelse med rettergang alene av den grunn at det er elektronisk.

KAPITTEL V

DELEGERING AV MYNDIGHET OG GJENNOMFØRINGSBESTEMMELSER

Artikkel 47

Utøvelse av delegert myndighet

1. Myndigheten til å vedta delegerte rettsakter gis Kommisjonen med forbehold for vilkårene fastsatt i denne artikkel.
2. Myndigheten til å vedta delegerte rettsakter nevnt i artikkel 30 nr. 4 gis Kommisjonen på ubestemt tid fra 17. september 2014.
3. Den delegerte myndigheten nevnt i artikkel 30 nr. 4 kan når som helst tilbakekalles av Europaparlamentet eller Rådet. En beslutning om tilbakekalling innebærer at den delegerte myndigheten som angis i beslutningen, opphører å gjelde. Beslutningen får anvendelse dagen etter at den er offentliggjort i *Den europeiske unions tidende*, eller på et senere tidspunkt angitt i beslutningen. Den berører ikke gyldigheten av delegerte rettsakter som allerede er trådt i kraft.
4. Så snart Kommisjonen vedtar en delegert rettsakt, skal den underrette Europaparlamentet og Rådet samtidig om dette.
5. En delegert rettsakt vedtatt i henhold til artikkel 30 nr. 4 skal tre i kraft bare dersom verken Europaparlamentet eller Rådet har gjort innsigelse mot rettsakten innen en frist på to måneder etter at rettsakten ble meddelt Europaparlamentet og Rådet, eller dersom både Europaparlamentet og Rådet innen utløpet av denne fristen har underrettet Kommisjonen om at de ikke kommer til å gjøre innsigelse. På Europaparlamentets eller Rådets initiativ forlenges denne fristen med to måneder.

Artikkel 48

Komitéframgangsmåte

1. Kommisjonen skal bistås av en komité. Nevnte komité skal være en komité i henhold til forordning (EU) nr. 182/2011.
2. Når det vises til dette nummer, får artikkel 5 i forordning (EU) nr. 182/2011 anvendelse.

KAPITTEL VI

SLUTTBESTEMMELSER

Artikkel 49

Gjennomgåelse

Kommisjonen skal gjennomgå anvendelsen av denne forordning og framlegge en rapport for Europaparlamentet og Rådet senest 1. juli 2020. Kommisjonen skal særlig vurdere om det er hensiktsmessig å endre denne forordnings virkeområde eller dens særlige bestemmelser, herunder artikkel 6, artikkel 7 bokstav f) og artikkel 34, 43, 44 og 45, idet det tas hensyn til erfaringene fra anvendelsen av denne forordning, den teknologiske og juridiske utvikling samt markedsutviklingen.

Rapporten nevnt i første ledd skal om nødvendig ledsages av forslag til regelverk.

Kommisjonen skal dessuten hvert fjerde år etter rapporten nevnt i første ledd framlegge en rapport for Europaparlamentet og Rådet om hvilke framskritt som er gjort med hensyn til å nå målene i denne forordning.

Artikkel 50

Oppheving

1. Direktiv 1999/93/EF oppheves med virkning fra 1. juli 2016.
2. Henvisninger til det opphevede direktivet skal forstås som henvisninger til denne forordning.

Artikkel 51

Overgangstiltak

1. Sikre signaturframstillingssystemer hvis samsvar er blitt fastslått i samsvar med artikkel 3 nr. 4 i direktiv 1999/93/EF, skal anses som kvalifiserte elektroniske signaturframstillingssystemer i henhold til denne forordning.
2. Kvalifiserte sertifikater utstedt til fysiske personer i henhold til direktiv 1999/93/EF skal anses som kvalifiserte sertifikater for elektroniske signaturer i henhold til denne forordning fram til de utløper.
3. En tilbyder av sertifiseringstjenester som utsteder kvalifiserte sertifikater i henhold til direktiv 1999/93/EF, skal framlegge en samsvarsvurderingsrap-

port for tilsynsorganet så snart som mulig og senest 1. juli 2017. Fram til en slik samsvarsvurderingsrapport er framlagt og tilsynsorganet har fullført sin vurdering av den, skal tilbyderen av sertifiseringstjenester anses som en kvalifisert tilbyder av tillitstjenester i henhold til denne forordning.

4. Dersom en tilbyder av sertifiseringstjenester som utsteder kvalifiserte sertifikater i henhold til direktiv 1999/93/EF, ikke framlegger en samsvarsvurderingsrapport for tilsynsorganet innen tidsfristen angitt i nr. 3, skal tilbyderen av sertifiseringstjenester ikke anses som en kvalifisert tilbyder av sertifiseringstjenester i henhold til denne forordning fra og med 2. juli 2017.

ARTIKKEL 52

IKRAFTTREDELSE

1. Denne forordning trer i kraft den 20. dagen etter at den er kunngjort i *Den europeiske unions tidende*.
2. Denne forordning får anvendelse fra 1. juli 2016, med unntak av følgende bestemmelser:
   a) Artikkel 8 nr. 3, 9 nr. 5, 12 nr. 2–9, 17 nr. 8, 19 nr. 4, 20 nr. 4, 21 nr. 4, 22 nr. 5, 23 nr. 3, 24 nr. 5, 27 nr. 4 og 5, 28 nr. 6, 29 nr. 2, 30 nr. 3 og 4, 31 nr. 3, 32 nr. 3, 33 nr. 2, 34 nr. 2, 37 nr. 4 og 5, 38 nr. 6, 42 nr. 2, 44 nr. 2, 45 nr. 2 og artikkel 47 og 48 får anvendelse fra 17. september 2014.
   b) Artikkel 7, artikkel 8 nr. 1 og 2, artikkel 9, 10, 11 og artikkel 12 nr. 1 får anvendelse fra anvendelsesdatoen for gjennomføringsrettsaktene nevnt i artikkel 8 nr. 3 og 12 nr. 8.
   c) Artikkel 6 får anvendelse fra og med tre år fra anvendelsesdatoen for gjennomføringsrettsaktene nevnt i artikkel 8 nr. 3 og 12 nr. 8.
3. Dersom den meldte ordningen for elektronisk identifikasjon er oppført på listen offentliggjort av Kommisjonen i henhold til artikkel 9 før datoen nevnt i nr. 2 bokstav c) i denne artikkel, skal de elektroniske identifikasjonsmidlene innenfor rammen av denne ordningen i henhold til artikkel 6 anerkjennes senest 12 måneder etter offentliggjøring av ordningen, men ikke før datoen nevnt i nr. 2 bokstav c) i denne artikkel.
4. Uten hensyn til nr. 2 bokstav c) i denne artikkel kan en medlemsstat beslutte at elektroniske identifikasjonsmidler innenfor rammen av en ordning for elektronisk identifikasjon som er meldt i henhold til artikkel 9 nr. 1 av en annen medlemsstat, skal anerkjennes i den første medlemsstaten fra og med anvendelsesdatoen for gjennomføringsrettsaktene nevnt i artikkel 8 nr. 3 og 12 nr. 8. De berørte medlemsstatene skal underrette Kommisjonen. Kommisjonen skal offentliggjøre disse opplysningene.

Denne forordning er bindende i alle deler og kommer direkte til anvendelse i alle medlemsstater.

Utferdiget i Brussel 23. juli 2014.

For Parlamentet

M. SCHULZ

President

For Rådet

S. GOZI

Formann

VEDLEGG I

KRAV TIL KVALIFISERTE SERTIFIKATER FOR ELEKTRONISKE SIGNATURER

Kvalifiserte sertifikater for elektroniske signaturer skal inneholde

a) en angivelse, som minst er i en form som er egnet for automatisert behandling, om at sertifikatet er utstedt som et kvalifisert sertifikat for elektronisk signatur,
b) et datasett som på en utvetydig måte representerer den kvalifiserte tilbyderen av tillitstjenester som utsteder de kvalifiserte sertifikatene, som minst inneholder opplysninger om hvilken medlemsstat tjenestetilbyderen er etablert i, og
   — for en juridisk person: navn og, når det er relevant, registreringsnummeret oppført i offisielle registre,
   — for en fysisk person: personens navn,
c) minst underskriverens navn eller et pseudonym, der pseudonymet er tydelig angitt dersom et slikt brukes,
d) valideringsdata for den elektroniske signaturen som stemmer overens med dataene for framstilling av den elektroniske signaturen,
e) opplysninger om når sertifikatets gyldighetsperiode starter og utløper,
f) sertifikatets identifikasjonskode, som må være entydig for den kvalifiserte tilbyderen av tillitstjenester,

g) den avanserte elektroniske signaturen eller det avanserte elektroniske seglet til den utstedende kvalifiserte tilbyderen av tillitstjenester,
h) opplysninger om hvor sertifikatet som støtter den avanserte elektroniske signaturen eller det avanserte elektroniske seglet nevnt i bokstav g), er gratis tilgjengelig,
i) opplysninger om hvor tjenestene som kan brukes for å få kjennskap til det kvalifiserte sertifikatets gyldighetsstatus, befinner seg,
j) dersom de elektroniske signaturframstillingsdataene som er knyttet til valideringsdataene for elektroniske signaturer, befinner seg i et kvalifisert elektronisk signaturframstillingssystem, en egnet angivelse av dette som minst skal være i en form som er egnet for automatisert behandling.

VEDLEGG II

KRAV TIL KVALIFISERTE ELEKTRONISKE SIGNATURFRAMSTILLINGSSYSTEMER

1. Kvalifiserte elektroniske signaturframstillingssystemer skal ved hjelp av egnede tekniske midler og framgangsmåter minst sikre at
   a) de elektroniske signaturframstillingsdataene som brukes til framstilling av elektroniske signaturer, behandles tilstrekkelig fortrolig,
   b) de elektroniske signaturframstillingsdataene som brukes til framstilling av elektroniske signaturer, i praksis kan forekomme bare én gang,
   c) de elektroniske signaturframstillingsdataene som brukes til framstilling av elektroniske signaturer, med rimelig sikkerhet ikke kan utledes, og at tilgjengelig teknologi er brukt for å beskytte den elektroniske signaturen mot forfalskning,
   d) den rettmessige underskriveren på en pålitelig måte kan hindre andre i å bruke de elektroniske signaturframstillingsdataene som brukes til framstilling av elektroniske signaturer.
2. Kvalifiserte elektroniske signaturframstillingssystemer skal ikke endre dataene som skal signeres, eller hindre at disse dataene vises for underskriveren før signaturprosessen.
3. Generering eller håndtering av elektroniske signaturframstillingsdata på vegne av underskriveren kan gjøres bare av en kvalifisert tilbyder av tillitstjenester.
4. Med forbehold for nr. 1 bokstav d) kan kvalifiserte tilbydere av tillitstjenester som håndterer elektroniske signaturframstillingsdata på vegne av underskriveren, kopiere disse dataene bare for å opprette sikkerhetskopier, forutsatt at følgende krav er oppfylt:
   a) sikkerhetsnivået for de kopierte datasettene må være det samme som for de opprinnelige datasettene,
   b) antall kopierte datasett skal ikke overskride minsteantallet som er nødvendig for å sikre kontinuitet i tjenesten.

VEDEGG III

KRAV TIL KVALIFISERTE SERTIFIKATER FOR ELEKTRONISKE SEGL

Kvalifiserte sertifikater for elektroniske segl skal inneholde

a) en angivelse, som minst er i en form som er egnet for automatisert behandling, om at sertifikatet er utstedt som et kvalifisert sertifikat for elektroniske segl,
b) et datasett som på en utvetydig måte representerer den kvalifiserte tilbyderen av tillitstjenester som utsteder de kvalifiserte sertifikatene, som minst inneholder opplysninger om hvilken medlemsstat tjenestetilbyderen er etablert i, og
   — for en juridisk person: navn og, når det er relevant, registreringsnummeret oppført i offisielle registre,
   — for en fysisk person: personens navn,
c) minst seglframstillerens navn og, når det er relevant, registreringsnummeret oppført i offisielle registre,
d) valideringsdata for det elektroniske seglet som stemmer overens med dataene for framstilling av det elektroniske seglet,
e) opplysninger om når sertifikatets gyldighetsperiode starter og utløper,
f) sertifikatets identifikasjonskode, som må være entydig for den kvalifiserte tilbyderen av tillitstjenester,
g) den avanserte elektroniske signaturen eller det avanserte elektroniske seglet til den utstedende kvalifiserte tilbyderen av tillitstjenester,
h) opplysninger om hvor sertifikatet som støtter den avanserte elektroniske signaturen eller det avanserte elektroniske seglet nevnt i bokstav g), er gratis tilgjengelig,
i) opplysninger om hvor tjenestene som kan brukes for å få kjennskap til det kvalifiserte sertifikatets gyldighetsstatus, befinner seg,
j) dersom de elektroniske seglframstillingsdataene som er knyttet til valideringsdataene for elektroniske segl, befinner seg i et system for framstilling av kvalifiserte elektroniske segl, en egnet angivelse av dette som minst skal være i en form som er egnet for automatisert behandling.

VEDLEGG IV

KRAV TIL KVALIFISERTE SERTIFIKATER FOR NETTSTEDAUTENTISERING

Kvalifiserte sertifikater for nettstedsautentisering skal inneholde

a) en angivelse, som minst er i en form som er egnet for automatisert behandling, om at sertifikatet er utstedt som et kvalifisert sertifikat for nettstedsautentisering,
b) et datasett som på en utvetydig måte representerer den kvalifiserte tilbyderen av tillitstjenester som utsteder de kvalifiserte sertifikatene, som minst inneholder opplysninger om hvilken medlemsstat tjenestetilbyderen er etablert i, og
   — for en juridisk person: navn og, når det er relevant, registreringsnummeret oppført i offisielle registre,
   — for en fysisk person: personens navn,
c) for fysiske personer: minst navnet på personen som sertifikatet er utstedt til, eller et pseudonym, der pseudonymet er tydelig angitt dersom et slikt brukes,

   for juridiske personer: minst navnet på den juridiske personen som sertifikatet er utstedt til, og eventuelt registreringsnummeret oppført i offisielle registre,
d) adresseopplysningene, herunder minst opplysninger om by og stat, til den fysiske eller juridiske personen som sertifikatet er utstedt til, og eventuelt som angitt i offisielle registre,
e) domenenavnet eller -navnene som drives av den fysiske eller juridiske personen som sertifikatet er utstedt til,
f) opplysninger om når sertifikatets gyldighetsperiode starter og utløper,
g) sertifikatets identifikasjonskode, som må være entydig for den kvalifiserte tilbyderen av tillitstjenester,
h) den avanserte elektroniske signaturen eller det avanserte elektroniske seglet til den utstedende kvalifiserte tilbyderen av tillitstjenester,
i) opplysninger om hvor sertifikatet som støtter den avanserte elektroniske signaturen eller det avanserte elektroniske seglet nevnt i bokstav h), er gratis tilgjengelig,
j) opplysninger om hvor tjenestene som kan brukes for å få kjennskap til det kvalifiserte sertifikatets gyldighetsstatus, befinner seg,

Svanemerketrykksak, 2041 0654 Trykk og layout: Stortingets grafiske seksjon