EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) Nr. 910/2014

af 23. juli 2014

om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 114,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg ([1]),

efter den almindelige lovgivningsprocedure ([2]), og

ud fra følgende betragtninger:

(1) Det er afgørende for den økonomiske og sociale udvikling, at der skabes tillid til onlineverdenen. Hvis tilliden mangler, især på grund af en formodning om manglende retssikkerhed, vil forbrugere, virksomheder og offentlige myndigheder tøve med at gennemføre transaktioner elektronisk og benytte nye tjenester.

(2) Denne forordning har til formål at styrke tilliden til elektroniske transaktioner på det indre marked ved at skabe et fælles grundlag for sikker elektronisk interaktion mellem borgere, virksomheder og offentlige myndigheder og derved øge effektiviteten i de offentlige og private onlinetjenester, elektronisk forretningsførelse og elektronisk handel i Unionen.

(3) Europa-Parlamentets og Rådets direktiv 1999/93/EF ([3]) dækkede elektroniske signaturer uden at skabe en omfattende ramme for sikre, pålidelige og brugervenlige elektroniske transaktioner på tværs af landegrænser og sektorer. Denne forordning styrker og udvider det nævnte direktivs regelsæt.

(4) I Kommissionens meddelelse af 26. august 2010 med titlen »En digital dagsorden for Europa« påpeges det, at opsplitningen af det digitale marked, manglende interoperabilitet og stigende internetkriminalitet er alvorlige hindringer for en positiv udvikling af den digitale økonomi. I sin rapport om unionsborgerskab fra 2010 med titlen »Afskaffelse af hindringerne for unionsborgernes rettigheder« fremhævede Kommissionen endvidere behovet for at løse de væsentligste problemer, der forhindrer EU-borgere i at nyde fordelene ved et digitalt indre marked og digitale tjenesteydelser på tværs af landegrænserne.

(5) Det Europæiske Råd opfordrede i sine konklusioner af 4. februar 2011 og af 23. oktober 2011 Kommissionen til at skabe et digitalt indre marked inden 2015 for at gøre hurtige fremskridt på nøgleområderne i den digitale økonomi og fremme et fuldt integreret digitalt indre marked ved at befordre brug af onlinetjenester på tværs af grænserne og lægge særlig vægt på at lette sikker elektronisk identifikation og autentifikation.

([1]) EUT C 351 af 15.11.2012, s. 73.
([2]) Europa-Parlamentets holdning af 3.4.2014 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 23.7.2014.
([3]) Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer (EFT L 13 af 19.1.2000, s. 12).

(6) Rådet opfordrede i sine konklusioner af 27. maj 2011 Kommissionen til at bidrage til det digitale indre marked ved at skabe passende vilkår for gensidig anerkendelse af centrale mulighedsskabende teknologier på tværs af grænserne, såsom elektronisk identifikation, elektroniske dokumenter, elektroniske signaturer og elektroniske leveringstjenester samt for interoperable e-forvaltningstjenester i hele Den Europæiske Union.

(7) Europa-Parlamentet understregede i sin beslutning af 21. september 2010 om gennemførelse af det indre marked for e-handel ([1]) betydningen af sikkerhed i forbindelse med elektroniske tjenester, navnlig elektroniske signaturer, samt af behovet for at etablere public key-infrastruktur på fælleseuropæisk plan, og det har opfordret Kommissionen til at etablere en gateway for europæiske valideringsmyndigheder for at sikre elektroniske signaturers grænseoverskridende interoperabilitet og øge sikkerheden for transaktioner, som foretages over internettet.

(8) Ifølge Europa-Parlamentets og Rådets direktiv 2006/123/EF ([2]) skal medlemsstaterne oprette »kvikskranker« for at sikre, at samtlige procedurer og formaliteter i forbindelse med adgangen til at optage og udøve servicevirksomhed kan afvikles uden besvær, på afstand og ad elektronisk vej via den berørte kvikskranke og de kompetente myndigheder. Mange af de onlinetjenester, der er tilgængelige via kvikskranker, kræver elektronisk identifikation, autentifikation og signatur.

(9) I de fleste tilfælde kan borgere ikke bruge deres elektroniske ID til at autentificere sig i en anden medlemsstat, fordi de nationale elektroniske identifikationsordninger i deres eget land ikke anerkendes i andre medlemsstater. Denne elektroniske hindring udelukker tjenesteudbyderne fra at høste det fulde udbytte af det indre marked. Gensidigt anerkendte elektroniske identifikationsmidler vil gøre det lettere at udbyde en lang række tjenester på tværs af grænserne på det indre marked og sætte virksomhederne i stand til at udøve virksomhed på tværs af grænserne uden at skulle overvinde diverse hindringer i kontakten med de offentlige myndigheder.

(10) Europa-Parlamentets og Rådets direktiv 2011/24/EU ([3]) etablerer et netværk mellem de nationale myndigheder, der er ansvarlige for e-sundhed. For at øge sikkerheden og kontinuiteten i forbindelse med grænseoverskridende sundhedsydelser skal netværket udarbejde retningslinjer for adgang til elektroniske sundhedsoplysninger og –ydelser på tværs af grænserne og blandt andet støtte »fælles identifikations- og autentifikationsforanstaltninger for at gøre det lettere at overføre data ved grænseoverskridende sundhedsydelser«. Gensidig anerkendelse af elektronisk identifikation og autentifikation er afgørende for, at sundhedsydelser for Europas borgere på tværs af grænserne bliver en realitet. Når borgerne tager til udlandet for at få lægebehandling, skal deres medicinske data være tilgængelige i det land, hvor de skal behandles. Dette kræver en solid og sikker ramme for elektronisk identifikation, som de berørte parter har tillid til.

(11) Denne forordning bør anvendes under fuld overholdelse af principperne vedrørende beskyttelse af personoplysninger i Europa-Parlamentets og Rådets direktiv 95/46/EF ([4]). For så vidt angår princippet om gensidig anerkendelse i denne forordning bør autentifikation i forbindelse med en onlinetjeneste derfor kun omfatte behandling af de identifikationsdata, der er tilstrækkelige, relevante og ikke omfatter mere, end hvad der kræves for at give adgang til den pågældende onlinetjeneste. Desuden bør tillidstjenesteudbydere og tilsynsorganer opfylde kravene i direktiv 95/46/EF om fortrolighed og behandlingssikkerhed.

(12) Et af formålene med denne forordning er at fjerne de eksisterende hindringer for grænseoverskridende brug af elektroniske identifikationsmidler, der benyttes i medlemsstaterne for som minimum at autentificere offentlige tjenester. Forordningen har ikke til formål at gribe ind for så vidt angår de elektroniske identitetsforvaltningssystemer og dermed forbundne infrastrukturer, der er etableret i medlemsstaterne. Målet med denne forordning er at sørge for, at der findes sikker elektronisk identifikation og autentifikation, der gør det muligt at få adgang til grænseoverskridende onlinetjenester, som medlemsstaterne udbyder.

([1]) EUT C 50 E af 21.2.2012, s. 1.
([2]) Europa-Parlamentets og Rådets direktiv 2006/123/EF af 12. december 2006 om tjenesteydelser i det indre marked (EUT L 376 af 27.12.2006, s. 36).
([3]) Europa-Parlamentets og Rådets direktiv 2011/24/EU af 9. marts 2011 om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser (EUT L 88 af 4.4.2011, s. 45).
([4]) Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT L 281 af 23.11.1995, s. 31).

(13) Medlemsstaterne bør fortsat frit kunne anvende eller indføre midler med henblik på elektronisk identifikation for adgang til onlinetjenester. De bør også selv kunne bestemme, om den private sektor skal være med til at udbyde disse midler. Medlemsstaterne bør ikke være forpligtet til at anmelde deres elektroniske identifikationsordninger til Kommissionen. Valget mellem at anmelde alle, nogle eller ingen af de elektroniske identifikationsordninger, der anvendes på nationalt plan til som minimum at få adgang til offentlige onlinetjenester eller specifikke tjenester, til Kommissionen bør være op til medlemsstaterne.

(14) Denne forordning bør indeholde visse betingelser for, hvilke elektroniske identifikationsmidler der skal anerkendes, og for, hvordan de elektroniske identifikationsordninger bør anmeldes. Betingelserne bør hjælpe medlemsstaterne til at opbygge den nødvendige tillid til hinandens elektroniske identifikationsordninger og til gensidigt at anerkende elektroniske identifikationsmidler, der er omfattet af de anmeldte ordninger. Princippet om gensidig anerkendelse bør følges, hvis den anmeldende medlemsstats elektroniske identifikationsordning opfylder anmeldelsesbetingelserne, og hvis anmeldelsen har været offentliggjort i *Den Europæiske Unions Tidende*. Dog bør princippet om gensidig anerkendelse kun gælde for autentifikation i forbindelse med en onlinetjeneste. Adgangen til disse onlinetjenester og den endelige levering af tjenesterne til parter, der anmoder herom, bør afhænge nøje af retten til at modtage sådanne tjenester i henhold til betingelserne i den nationale lovgivning.

(15) Pligten til at anerkende elektroniske identifikationsmidler bør kun vedrøre de midler, hvis identitetssikringsniveau svarer til eller er højere end det niveau, der kræves for den pågældende onlinetjeneste. Desuden bør pligten kun gælde, når den pågældende offentlige myndighed anvender sikringsniveauet »betydelig« eller »høj« i forbindelse med adgang til den pågældende onlinetjeneste. Medlemsstaterne bør i overensstemmelse med EU-retten frit kunne anerkende elektroniske identifikationsmidler, der har lavere identitetssikringsniveauer.

(16) Sikringsniveauer bør afspejle graden af tillid til, at et elektronisk identifikationsmiddel kan fastslå identiteten på en person og således give sikkerhed for, at den person, der gør krav på en specifik identitet, faktisk er den person, hvortil identiteten er blevet knyttet. Sikringsniveauet afhænger af graden af tillid til, at det elektroniske identifikationsmiddel kan fastslå en persons påståede identitet, idet der tages hensyn til processer (for eksempel godtgørelse, kontrol og autentifikation af identitet), ledelsesaktiviteter (for eksempel den enhed, der udsteder det elektroniske identifikationsmiddel, og proceduren for udstedelse af sådanne midler) og iværksatte tekniske kontroller. Der eksisterer forskellige tekniske definitioner på og beskrivelser af sikringsniveauer som følge af EU-finansierede pilotprojekter i stor skala, standardiseringer og internationale aktiviteter. Navnlig i pilotprojekterne i stor skala STORK og ISO 29115 henvises der blandt andet til niveauerne 2, 3 og 4, som der bør tages størst muligt hensyn til ved fastsættelsen af tekniske minimumskrav, standarder og procedurer for sikringsniveauerne »lav«, »betydelig« og »høj« som omhandlet i denne forordning, samtidig med at der sikres ensartet anvendelse af denne forordning, især hvad angår sikringsniveauet »høj« i forbindelse med godtgørelse af identitet ved udstedelsen af kvalificerede certifikater. De fastsatte krav bør være teknologineutrale. Det bør være muligt at opfylde de nødvendige sikkerhedskrav med forskellige teknologier.

(17) Medlemsstaterne bør tilskynde den private sektor til frivilligt at anvende elektroniske identifikationsmidler, der er omfattet af en anmeldt ordning, til identifikationsformål, når dette er nødvendigt med henblik på onlinetjenester eller elektroniske transaktioner. Muligheden for at anvende sådanne elektroniske identifikationsmidler vil betyde, at den private sektor kan benytte sig af elektronisk identifikation og autentifikation, der allerede anvendes i vid udstrækning i mange medlemsstater, i det mindste til offentlige tjenester, og gøre det lettere for virksomhederne og borgerne at få adgang til deres onlinetjenester på tværs af grænserne. For at gøre det lettere for den private sektor at bruge sådanne elektroniske identifikationsmidler på tværs af grænserne bør den autentifikationsmulighed, som en medlemsstat udbyder, stilles til rådighed for modtagerparter i den private sektor, der er hjemmehørende uden for medlemsstatens område, på samme betingelser, som gælder for modtagerparter i den private sektor, der er hjemmehørende i medlemsstaten. Med hensyn til modtagerparter i den private sektor kan den anmeldende medlemsstat fastsætte betingelser for adgang til autentifikationsmidlerne. Disse adgangsbetingelser kan omfatte oplysninger om, at autentifikationsmidlerne i tilknytning til den anmeldte ordning ikke i øjeblikket er til rådighed for modtagerparter i den private sektor.

(18) Denne forordning bør fastsætte det erstatningsansvar, der påhviler den anmeldende medlemsstat, den part, der udsteder det elektroniske identifikationsmiddel, og den part, der udfører autentifikationsproceduren, hvis de ikke opfylder de relevante forpligtelser i henhold til denne forordning. Denne forordning bør imidlertid anvendes i overensstemmelse med nationale regler om erstatningsansvar. Derfor berører den ikke de nationale regler, der handler om f.eks. definition af skadeserstatning eller relevante gældende procedureregler, herunder bevisbyrden.

(19) Sikkerheden i ordninger for elektronisk identifikation er central i en pålidelig grænseoverskridende gensidig anerkendelse af elektroniske identifikationsmidler. I den forbindelse bør medlemsstaterne samarbejde om sikkerhed og interoperabilitet i ordningerne for elektronisk identifikation på EU-plan. Når det i ordningerne for elektronisk identifikation kræves, at modtagerparter skal anvende bestemt hardware eller software på nationalt plan, indebærer grænseoverskridende interoperabilitet, at disse medlemsstater ikke må pålægge modtagerparter, der er hjemmehørende uden for deres område, sådanne krav og dermed forbundne omkostninger. I så fald bør passende løsninger drøftes og udformes inden for interoperabilitetsrammen. Dog er tekniske krav, der hidrører fra de iboende specifikationer for nationale elektroniske identifikationsmidler, og som kan berøre indehaverne af sådanne elektroniske midler (f.eks. smartkort), uundgåelige.

(20) Samarbejdet mellem medlemsstaterne bør lette den tekniske interoperabilitet mellem de anmeldte elektroniske identifikationsordninger med henblik på at bidrage til et højt niveau af tillid og sikkerhed, der står i et passende forhold til risikoen. Udveksling af information og bedste praksis mellem medlemsstaterne med henblik på gensidig anerkendelse af identifikationsordningerne bør fremme et sådant samarbejde.

(21) Denne forordning bør også fastlægge en generel lovramme for brug af tillidstjenester. Der bør dog ikke indføres en generel pligt til at bruge dem eller til at oprette et adgangspunkt for alle eksisterende tillidstjenester. Den bør navnlig ikke omfatte levering af tjenester, der udelukkende anvendes i lukkede systemer mellem et defineret sæt deltagere, der ikke har virkning over for tredjemand. For eksempel bør systemer, der er oprettet i virksomheder eller offentlige forvaltninger til styring af interne procedurer ved brug af tillidstjenester, ikke være omfattet af kravene i denne forordning. Kun tillidstjenester, der udbydes til offentligheden, og som har virkning over for tredjemand, bør opfylde kravene i denne forordning. Denne forordning bør heller ikke omfatte aspekter i forbindelse med indgåelse og gyldighed af kontrakter eller andre retlige forpligtelser, som ifølge national ret eller EU-ret er undergivet formkrav. Den bør heller ikke berøre nationale formkrav til offentlige registre, navnlig handelsregistre og tingbøger.

(22) For at bidrage til deres udbredte brug på tværs af grænserne bør det være muligt at bruge tillidstjenester som bevis i retssager i alle medlemsstater. Retsvirkningerne af tillidstjenester i medlemsstaterne defineres i national ret, medmindre andet er fastsat i denne forordning.

(23) I det omfang denne forordning indfører en pligt til at anerkende en tillidstjeneste, kan denne tillidstjeneste kun afvises, hvis den, som pligten er rettet mod, af tekniske grunde, som vedkommende ikke har nogen umiddelbar indflydelse på, ikke kan læse eller kontrollere den. Pligten bør dog ikke i sig selv indebære, at et offentligt organ skal skaffe den hardware eller software, der er nødvendig for den tekniske læsbarhed af alle eksisterende tillidstjenester.

(24) Medlemsstaterne kan i overensstemmelse med EU-retten opretholde eller indføre nationale bestemmelser vedrørende tillidstjenester, for så vidt disse tjenester ikke er fuldt harmoniseret ved denne forordning. Der er dog fri bevægelighed på det indre marked for tillidstjenester, der overholder bestemmelserne i denne forordning.

(25) Det bør stå medlemsstaterne frit for at fastlægge andre typer tillidstjenester ud over dem, der indgår i den lukkede liste over tillidstjenester, der er omfattet af denne forordning, med henblik på at anerkende dem på nationalt plan som kvalificerede tillidstjenester.

(26) I betragtning af den hurtige teknologiske udvikling bør denne forordning følge en fremgangsmåde, der er åben over for innovation.

(27) Denne forordning bør være teknologineutral. De retsvirkninger, den giver, bør kunne opnås ved et hvilket som helst teknisk middel, forudsat at kravene i denne forordning er opfyldt.

(28) For at styrke især de små og mellemstore virksomheders (SMV'er) og forbrugernes tillid til det indre marked og fremme brugen af tillidstjenester og -produkter bør begreberne kvalificerede tillidstjenester og kvalificeret tillidstjenesteudbyder indføres med henblik på at opstille krav og forpligtelser, der skal sikre et højt niveau af sikkerhed for alle de tillidstjenester og –produkter, der benyttes eller udbydes.

(29) I overensstemmelse med forpligtelserne i De Forenede Nationers konvention om handicappedes rettigheder, der blev godkendt ved Rådets afgørelse 2010/48/EF ([1]), særlig artikel 9 i konventionen, bør handicappede have mulighed for at benytte tillidstjenester og slutbrugerprodukter, der bruges til levering af disse tjenester, på lige fod med andre forbrugere. Derfor bør tillidstjenester og slutbrugerprodukter, der bruges til levering af disse tjenester, så vidt muligt være tilgængelige for handicappede. Gennemførlighedsvurderingen bør bl.a. omfatte tekniske og økonomiske hensyn.

(30) Medlemsstaterne bør udpege et eller flere tilsynsorganer til at udføre tilsynsvirksomhed i henhold til denne forordning. Medlemsstaterne bør også efter gensidig aftale med en anden medlemsstat kunne beslutte at udpege et tilsynsorgan på den anden medlemsstats område.

(31) Tilsynsorganerne bør samarbejde med databeskyttelsesmyndighederne, f.eks. ved at underrette dem om resultaterne af revisioner af kvalificerede tillidstjenesteudbydere, når der er mistanke om overtrædelse af reglerne om beskyttelse af personoplysninger. Underretningen bør navnlig omfatte sikkerhedsrelaterede hændelser og brud på persondatasikkerheden.

(32) For at styrke brugernes tillid til det indre marked bør det påhvile alle tillidstjenesteudbydere at følge en god sikkerhedspraksis, som er afpasset efter de risici, der er forbundet med deres aktiviteter.

(33) Bestemmelserne om brug af pseudonymer i certifikater bør ikke forhindre medlemsstaterne i at stille krav om identifikation af personer i henhold til EU-ret eller national ret.

(34) Alle medlemsstater bør følge fælles væsentlige tilsynskrav, så der tilvejebringes et ensartet sikkerhedsniveau for kvalificerede tillidstjenester. For at bidrage til en ensartet anvendelse af disse krav i hele Unionen bør medlemsstaterne indføre sammenlignelige procedurer og udveksle information om deres tilsynsvirksomhed og om bedste praksis på området.

(35) Alle tillidstjenesteudbydere bør være omfattet af kravene i denne forordning, navnlig hvad angår sikkerhed og erstatningsansvar for at sikre, at der udvises nødvendig omhu, gennemsigtighed og ansvarlighed i forbindelse med deres operationer og tjenester. Under hensyn til den type tjenester, som tillidstjenesteudbydere udbyder, er det imidlertid hensigtsmæssigt for disse kravs vedkommende at skelne mellem kvalificerede og ikkekvalificerede tillidstjenesteudbydere.

(36) Indførelse af en tilsynsordning for alle tillidstjenesteudbydere skulle sikre lige vilkår for deres operationers og tjenesters sikkerhed og ansvarlighed og dermed bidrage til beskyttelsen af brugerne og til det indre markeds funktion. Ikkekvalificerede tillidstjenesteudbydere bør underkastes et let og reaktivt efterfølgende tilsyn under hensyn til arten af deres tjenester og operationer. Tilsynsorganet bør således ikke have en generel pligt til at føre tilsyn med ikkekvalificerede tjenesteudbydere. Tilsynsorganet bør kun skride til handling, når det bliver underrettet (f.eks. af den ikkekvalificerede tillidstjenesteudbyder selv, af et andet tilsynsorgan, ved en anmeldelse fra en bruger eller forretningspartner eller på grundlag af sin egen efterforskning) om, at en ikkekvalificeret tillidstjenesteudbyder ikke opfylder denne forordnings krav.

([1]) Rådets afgørelse 2010/48/EF af 26. november 2009 om Det Europæiske Fællesskabs indgåelse af De Forenede Nationers konvention om handicappedes rettigheder (EUT L 23 af 27.1.2010, s. 35).

(37) Denne forordning bør fastsætte alle tillidstjenesteudbyderes erstatningsansvar. Den indfører navnlig en erstatningsansvarsordning, hvorefter alle tillidstjenesteudbydere bør være erstatningsansvarlige for skader forvoldt mod en fysisk eller juridisk person på grund af manglende opfyldelse af denne forordnings forpligtelser. For at lette vurderingen af de økonomiske risici, som tillidstjenesteudbydere måske skal bære, eller som de bør forsikre sig imod, giver denne forordning tillidstjenesteudbydere mulighed for på visse betingelser at fastsætte begrænsninger i brugen af de tjenester, som de udbyder, og for at fralægge sig erstatningsansvaret for skader som følge af en brug af tjenesterne, der går videre end disse begrænsninger. Kunderne bør underrettes behørigt om begrænsningerne på forhånd. Disse begrænsninger bør være klare for en tredjepart, f.eks. ved oplysninger om begrænsningerne i vilkårene for den ydede tjeneste eller på andre tydelige måder. Med henblik på at gennemføre disse principper bør denne forordning anvendes i overensstemmelse med de nationale bestemmelser om erstatningsansvar. Denne forordning berører derfor ikke disse nationale bestemmelser om f.eks. definition af skadeserstatning, forsæt, uagtsomhed eller relevante gældende procedurebestemmelser.

(38) Det er afgørende, at brud på sikkerheden og sikkerhedsrisikovurderinger indberettes, så de berørte parter får fyldestgørende oplysninger i tilfælde af brud på sikkerheden eller tab af integritet.

(39) For at Kommissionen og medlemsstaterne kan vurdere effektiviteten af den ordning for indberetning af brud på sikkerheden, der indføres ved denne forordning, bør tilsynsorganerne anmodes om at forelægge sammenfattende oplysninger for Kommissionen og Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA).

(40) For at Kommissionen og medlemsstaterne kan vurdere effektiviteten af den forbedrede tilsynsordning, der indføres ved denne forordning, bør tilsynsorganerne anmodes om at aflægge rapport om deres aktiviteter. Dette vil fremme udvekslingen af god praksis mellem tilsynsorganerne og lette kontrollen af, at de væsentlige tilsynskrav gennemføres ensartet og effektivt i alle medlemsstater.

(41) For at garantere kvalificerede tillidstjenesters bæredygtighed og holdbarhed og styrke brugernes tillid til disse tjenesters kontinuitet bør tilsynsorganerne kontrollere, om der findes bestemmelser om planer for virksomhedsafbrydelse, og om de anvendes korrekt, i tilfælde hvor kvalificerede tillidstjenesteudbydere ophører med deres virksomhed.

(42) For at lette tilsynet med kvalificerede tillidstjenesteudbydere, for eksempel når en udbyder udbyder tjenester på en anden medlemsstats område og ikke er underkastet tilsyn der, eller når en udbyders computere befinder sig i en anden medlemsstat end den, hvor udbyderen er hjemmehørende, bør der indføres en ordning for gensidig bistand mellem tilsynsorganerne i medlemsstaterne.

(43) For at sikre, at kvalificerede tillidstjenesteudbydere og de tjenester, de udbyder, opfylder kravene i denne forordning, bør et overensstemmelsesvurderingsorgan foretage en overensstemmelsesvurdering, og de kvalificerede tillidstjenesteudbydere bør forelægge tilsynsorganet de overensstemmelsesvurderingsrapporter, der herefter udarbejdes. Når tilsynsorganet kræver, at en kvalificeret tillidstjenesteudbyder forelægger en ad hoc-overensstemmelsesvurderingsrapport, bør tilsynsorganet især overholde princippet om god forvaltningspraksis, herunder pligten til at begrunde sine beslutninger, og proportionalitetsprincippet. Derfor bør tilsynsorganet behørigt begrunde sin beslutning om at kræve en ad hoc-overensstemmelsesvurdering.

(44) Denne forordning har til formål at sikre en sammenhængende ramme med henblik på at opnå et højt sikkerheds- og retssikkerhedsniveau i tillidstjenester. Når Kommissionen behandler overensstemmelsesvurderingen af produkter og tjenester, bør den derfor, når det er hensigtsmæssigt, søge synergier med gældende relevante europæiske og internationale ordninger såsom Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 ([1]), som fastlægger kravene til akkreditering af overensstemmelsesvurderingsorganer og markedsovervågning af produkter.

([1]) Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 af 9. juli 2008 om kravene til akkreditering og markedsovervågning i forbindelse med markedsføring af produkter og om ophævelse af forordning (EØF) nr. 339/93 (EUT L 218 af 13.8.2008, s. 30).

(45) For at tillade en effektiv iværksættelsesproces, der bør føre til, at kvalificerede tillidstjenesteudbydere og deres kvalificerede tillidstjenester optages på positivlister, bør der tilskyndes til indledende kontakter mellem eventuelle fremtidige kvalificerede tillidstjenesteudbydere og de kompetente tilsynsorganer med det formål at fremme den nødvendige omhu, der er forudsætningen for levering af kvalificerede tillidstjenester.

(46) Positivlister er afgørende elementer for at opbygge tillid blandt markedsaktørerne, da de fastslår tjenesteudbyderens status som kvalificeret udbyder på tidspunktet for tilsyn.

(47) Tillid til og bekvemmelighed i forbindelse med onlinetjenester er afgørende elementer for brugerne, så de kan høste det fulde udbytte og bevidst benytte elektroniske tjenester. Med henblik herpå bør der indføres et EU-tillidsmærke for at udpege de kvalificerede tillidstjenester, som kvalificerede tillidstjenesteudbydere udbyder. Et sådant EU-tillidsmærke for kvalificerede tillidstjenester vil klart skelne mellem kvalificerede tillidstjenester og andre tillidstjenester og således bidrage til gennemsigtighed på markedet. De kvalificerede tillidstjenesteudbyderes anvendelse af et EU-tillidsmærke bør være frivillig og bør ikke medføre andre krav end dem, der allerede er fastsat i denne forordning.

(48) Et højt sikkerhedsniveau er nødvendigt for at sikre gensidig anerkendelse af elektroniske signaturer, men i særlige tilfælde, f.eks. i forbindelse med Kommissionens beslutning 2009/767/EF [1], bør der også accepteres elektroniske signaturer med et lavere sikringsniveau.

(49) Denne forordning bør fastsætte princippet om, at en elektronisk signatur ikke må nægtes retsvirkning, alene af den grund at den er i elektronisk form, eller at den ikke opfylder alle kravene til en kvalificeret elektronisk signatur. Imidlertid fastsættes elektroniske signaturers retsvirkning i national ret, bortset fra kravene i denne forordning om, at en kvalificeret elektronisk signatur skal have samme retsvirkning som en håndskreven underskrift.

(50) Da de kompetente myndigheder i medlemsstaterne i øjeblikket benytter forskellige formater for avancerede elektroniske signaturer til at underskrive deres dokumenter elektronisk, er det nødvendigt at sørge for, at medlemsstaterne teknisk kan understøtte i det mindste et vist antal formater for avancerede elektroniske signaturer, når de modtager dokumenter, der er underskrevet elektronisk. Tilsvarende er det nødvendigt at sørge for, at de kompetente myndigheder i medlemsstaterne, når de anvender avancerede elektroniske segl, understøtter i det mindste et vist antal formater for avancerede elektroniske segl.

(51) Det bør være muligt for underskriveren at overdrage et kvalificeret elektronisk signaturgenereringssystem til tredjemands varetægt, forudsat at der anvendes passende mekanismer og procedurer til at sikre, at underskriveren bevarer fuld kontrol over brugen af sine elektroniske signaturgenereringsdata, og at brugen af systemet opfylder kravene til kvalificerede elektroniske signaturer.

(52) Genereringen af elektroniske signaturer på afstand, hvor miljøet til elektronisk signaturgenerering forvaltes af en tillidstjenesteudbyder på vegne af underskriveren, forventes at udvikle sig på grund af de mange økonomiske fordele forbundet hermed. Med henblik på at sikre, at sådanne elektroniske signaturer opnår samme juridiske anerkendelse som elektroniske signaturer, der genereres ved hjælp af et miljø, der fuldt ud forvaltes af brugeren, skal de udbydere, der udbyder elektroniske signaturtjenester på afstand, dog anvende specifikke ledelsesmæssige og administrative sikkerhedsprocedurer og benytte pålidelige systemer og produkter, herunder sikre elektroniske kommunikationskanaler, med henblik på at sikre, at miljøet for elektronisk signaturgenerering er pålideligt, og at det udelukkende anvendes under underskriverens enekontrol. Hvis en kvalificeret elektronisk signatur er blevet genereret ved hjælp af et system til generering af elektroniske signaturer på afstand, bør de gældende krav til de kvalificerede tillidstjenesteudbydere i denne forordning finde anvendelse.

[1] Kommissionens beslutning 2009/767/EF af 16. oktober 2009 om fastlæggelse af foranstaltninger, der skal lette anvendelsen af elektroniske procedurer ved hjælp af kvikskranker i henhold til Europa-Parlamentets og Rådets direktiv 2006/123/EF om tjenesteydelser i det indre marked (EUT L 274 af 20.10.2009, s. 36).

(53) Suspensionen af kvalificerede certifikater er en etableret praksis blandt tillidstjenesteudbydere i en række medlemsstater, som adskiller sig fra spærring, og som medfører midlertidigt tab af et certifikats gyldighed. Af hensyn til retssikkerheden kræves det, at et certifikats suspensionsstatus altid angives klart. Derfor bør tillidstjenesteudbydere have ansvaret for klart at angive certifikatets status og, såfremt det er suspenderet, angive den præcise suspensionsperiode. Denne forordning bør ikke pålægge tillidstjenesteudbyderne eller medlemsstaterne at anvende suspension, men fastlægge gennemsigtighedsbestemmelser, når og hvor en sådan praksis findes.

(54) Kvalificerede certifikaters grænseoverskridende interoperabilitet og anerkendelse er en forudsætning for kvalificerede elektroniske signaturers grænseoverskridende anerkendelse. Kvalificerede certifikater bør derfor ikke underlægges ufravigelige krav, der går videre end kravene i denne forordning. På nationalt plan bør det dog være tilladt at medtage særlige kendetegn såsom entydige identifikatorer i kvalificerede certifikater, hvis de særlige kendetegn ikke hindrer kvalificerede certifikaters og elektroniske signaturers grænseoverskridende interoperabilitet og anerkendelse.

(55) IT-sikkerhedscertificering baseret på internationale standarder som f.eks. ISO 15408 og dertil knyttede evalueringsmetoder og gensidige anerkendelsesordninger er et vigtigt redskab til at kontrollere sikkerheden af kvalificerede elektroniske signaturgenereringssystemer og bør fremmes. Innovative løsninger og tjenester som f.eks. mobil signatur, cloudsignatur benytter imidlertid tekniske og organisatoriske løsninger for kvalificerede elektroniske signaturgenereringssystemer, hvortil der eventuelt endnu ikke findes tilgængelige sikkerhedsstandarder, eller for hvilke den første IT-sikkerhedscertificering ikke er afsluttet. Kun i de tilfælde, hvor sådanne sikkerhedsstandarder ikke er tilgængelige, eller hvor den første IT-sikkerhedscertificering ikke er afsluttet, vil sikkerhedsniveauet for sådanne kvalificerede elektroniske signaturgenereringssystemer kunne evalueres under anvendelse af alternative processer. Disse processer bør være sammenlignelige med standarder for IT-sikkerhedscertificering, i det omfang deres sikkerhedsniveauer er ens. En fagfællebedømmelse (peer review) vil kunne lette disse processer.

(56) Denne forordning bør indeholde krav til kvalificerede elektroniske signaturgenereringssystemer, som skal sikre, at avancerede elektroniske signaturer fungerer hensigtsmæssigt. Denne forordning bør ikke omfatte det samlede omgivende miljø, som systemerne opererer i. Certificeringen af kvalificerede signaturgenereringssystemer bør derfor begrænses til hardware og software, der anvendes til at forvalte og beskytte de signaturgenereringsdata, der genereres, lagres eller behandles i signaturgenereringssystemet. Som anført i de relevante standarder bør certificeringspligten ikke omfatte applikationer til generering af signaturer.

(57) For at sikre retssikkerhed for så vidt angår signaturens gyldighed er det nødvendigt at specificere, hvilke elementer af en kvalificeret elektronisk signatur der bør vurderes af den modtagerpart, der foretager valideringen. Desuden bør fastlæggelsen af krav til kvalificerede tillidstjenesteudbydere, der kan udbyde en kvalificeret valideringstjeneste til modtagerparter, som ikke ønsker eller er i stand til selv at validere kvalificerede elektroniske signaturer, tilskynde den private og den offentlige sektor til at investere i sådanne tjenester. Tilsammen burde disse elementer gøre det nemt og bekvemt for alle parter at validere kvalificerede elektroniske signaturer på EU-plan.

(58) Når en transaktion kræver en juridisk persons kvalificerede elektroniske segl, bør en kvalificeret elektronisk signatur tilhørende den juridiske persons bemyndigede repræsentant, også accepteres.

(59) Et elektronisk segl bør tjene som bevis for, at et elektronisk dokument er udstedt af en juridisk person, og give sikkerhed for dokumentets oprindelse og integritet.

(60) Tillidstjenesteudbydere, der udsteder kvalificerede certifikater for elektroniske segl, bør anvende de nødvendige foranstaltninger til at fastslå identiteten på den fysiske person, der repræsenterer den juridiske person, som det kvalificerede certifikat for elektronisk segl udstedes til, når denne identifikation er nødvendig på nationalt plan som led i retlig eller administrativ forfølgning.

(61) Denne forordning bør sikre langtidsopbevaring af information, for at sikre at elektroniske signaturer og elektroniske segl har retsgyldighed over et længere tidsrum, og garantere, at de kan valideres uanset fremtidige teknologiske ændringer.

(62) Med henblik på at garantere kvalificerede elektroniske tidsstemplers sikkerhed bør denne forordning kræve, at der anvendes et avanceret elektronisk segl eller en avanceret elektronisk signatur eller andre tilsvarende metoder. Det kan forventes, at innovation kan føre til nye teknologier, som kan sikre et tilsvarende sikkerhedsniveau for tidsstempler. Når der anvendes en anden metode end avancerede elektroniske segl eller avancerede elektroniske signaturer, bør det påhvile den kvalificerede tillidstjenesteudbyder i overensstemmelsesvurderingsrapporten at godtgøre, at denne metode giver et tilsvarende sikkerhedsniveau og opfylder forpligtelserne i denne forordning.

(63) Elektroniske dokumenter er vigtige for den videre udvikling af grænseoverskridende elektroniske transaktioner på det indre marked. Denne forordning bør fastsætte princippet om, at et elektronisk dokument ikke må nægtes retsvirkning af den grund, at det er i elektronisk form, for at sikre, at en elektronisk transaktion ikke afvises, alene af den grund at et dokument foreligger i elektronisk form.

(64) Når Kommissionen behandler formaterne for avancerede elektroniske signaturer og segl, bør den tage udgangspunkt i eksisterende praksis, standarder og lovgivning, især Kommissionens afgørelse 2011/130/EU ([1]).

(65) Ud over at kunne bruges til autentifikation af dokumenter, der er udstedt af en juridisk person, kan elektroniske segl bruges til at autentificere alle den juridiske persons digitale aktiver, som f.eks. softwarekode eller servere.

(66) Det er vigtigt at fastlægge en retlig ramme for at lette grænseoverskridende anerkendelse mellem eksisterende nationale retsregler vedrørende elektroniske registrerede leveringstjenester. Denne ramme vil også kunne åbne nye markedsmuligheder for tillidstjenesteudbydere i Unionen med hensyn til at udbyde nye fælleseuropæiske tjenester for elektroniske registrerede leveringstjenester.

(67) Webstedsautentifikationstjenester giver besøgende på et websted sikkerhed for, at der står en ægte og legitim enhed bag webstedet. Disse tjenester bidrager til at opbygge tilliden i forbindelse med onlineforretninger, da brugerne vil have tillid til et websted, som er autentificeret. Ydelse og brug af webstedsautentifikationstjenester er helt frivillig. For at webstedsautentifikation kan blive et middel til at fremme tilliden ved at give brugerne en bedre oplevelse og stimulere vækst på det indre marked bør denne forordning dog fastlægge minimumsforpligtelser for tjenesteudbyderne og deres tjenester med hensyn til sikkerhed og erstatningsansvar. Med henblik herpå er der taget hensyn til resultaterne af igangværende industriledede initiativer, f.eks. Certification Authorities/Browser Forum — CA/Browser Forum. Desuden bør denne forordning ikke hindre brugen af andre midler eller metoder til autentifikation af et websted, der ikke er omfattet af denne forordning, og bør heller ikke forhindre ydere af webstedsautentifikationstjenester i tredjelande i at yde deres tjenester til kunder i Unionen. En tjenesteudbyder i et tredjeland bør dog kun kunne få sine webstedsautentifikationstjenester anerkendt som kvalificerede i overensstemmelse med denne forordning, hvis der er indgået en international aftale mellem Unionen og det land, hvor tjenesteudbyderen er hjemmehørende.

(68) Begrebet »juridiske personer« i henhold til bestemmelserne i traktaten om Den Europæiske Unions funktionsmåde (TEUF) om etablering giver operatørerne mulighed for frit at vælge den retlige form, de måtte finde passende for udøvelsen af deres virksomhed. Begrebet »juridiske personer« i henhold til TEUF omfatter derfor alle enheder, der er oprettet i henhold til eller reguleret af en medlemsstats ret, uanset deres retlige form.

(69) EU-institutionerne, -organerne, -kontorerne og -agenturerne opfordres til at anerkende elektronisk identifikation og tillidstjenester dækket af denne forordning med henblik på administrativt samarbejde, der især udnytter eksisterende god praksis og resultaterne af igangværende projekter på de områder, der er dækket af denne forordning.

([1]) Kommissionens afgørelse 2011/130/EU af 25. februar 2011 om fastsættelse af mindstekrav ved behandling af elektronisk underskrevne dokumenter på tværs af grænserne foretaget af de kompetente myndigheder som omhandlet i Europa-Parlamentets og Rådets direktiv 2006/123/EF om tjenesteydelser i det indre marked (EUT L 53 af 26.2.2011, s. 66).

(70) For at supplere visse detaljerede tekniske aspekter af denne forordning på fleksibel og hurtig vis, bør beføjelsen til at vedtage retsakter delegeres til Kommissionen i overensstemmelse med artikel 290 i TEUF, for så vidt angår de kriterier, som de organer, der er ansvarlige for certificering af kvalificerede elektroniske signaturgenereringssystemer, skal opfylde. Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau. Kommissionen bør i forbindelse med forberedelsen og udarbejdelsen af delegerede retsakter sørge for samtidig, rettidig og hensigtsmæssig fremsendelse af relevante dokumenter til Europa-Parlamentet og Rådet.

(71) For at sikre ensartede betingelser for gennemførelsen af denne forordning bør Kommissionen tillægges gennemførelsesbeføjelser, navnlig beføjelse til at opstille referencenumre på standarder, hvis anvendelse ville skabe formodning om overensstemmelse med bestemte krav, der er fastlagt i denne forordning. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 ([1]).

(72) Når Kommissionen vedtager delegerede retsakter eller gennemførelsesretsakter, bør den tage behørigt hensyn til de standarder og tekniske specifikationer, som europæiske og internationale standardiseringsorganisationer og organer har udarbejdet, navnlig Den Europæiske Standardiseringsorganisation (CEN), Det Europæiske Institut for Telestandarder (ETSI), Den Internationale Standardiseringsorganisation (ISO) og Den Internationale Telekommunikationsunion (ITU), for at sikre et højt sikkerheds- og interoperabilitetsniveau for elektroniske identifikations- og tillidstjenester.

(73) Af hensyn til retssikkerheden og klarheden bør direktiv 1999/93/EF ophæves.

(74) Af hensyn til retssikkerheden for de markedsoperatører, der allerede benytter kvalificerede certifikater, som er udstedt til fysiske personer i overensstemmelse med direktiv 1999/93/EF, er det nødvendigt at foreskrive en tilstrækkelig overgangsperiode. På samme måde bør der fastlægges overgangsforanstaltninger for sikre signaturgenereringssystemer, hvis opfyldelse af kravene er fastslået i overensstemmelse med direktiv 1999/93/EF, og for certificeringstjenesteudbydere, der udsteder kvalificerede certifikater inden den 1. juli 2016. Endelig er det også nødvendigt at give Kommissionen beføjelser til at vedtage gennemførelsesretsakter og delegerede retsakter før udløbet af overgangsperioden.

(75) Anvendelsesdatoerne i denne forordning berører ikke eksisterende forpligtelser, som medlemsstaterne allerede har indgået i henhold til EU-retten, navnlig i henhold til direktiv 2006/123/EF.

(76) Målene for denne forordning kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af foranstaltningens omfang bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke videre, end hvad der er nødvendigt for at nå disse mål.

(77) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 28, stk. 2, i Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 ([2]) og har afgivet en udtalelse den 27. september 2012 ([3]) —

([1]) Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser (EUT L 55 af 28.2.2011, s. 13).

([2]) Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger (EUT L 8 af 12.1.2001, s. 1).

([3]) EUT C 28 af 30.1.2013, s. 6.

VEDTAGET DENNE FORORDNING:

KAPITEL I

ALMINDELIGE BESTEMMELSER

Artikel 1

Genstand

Med henblik på at sikre et velfungerende indre marked, samtidig med at der sigtes mod et tilstrækkeligt sikkerhedsniveau for elektroniske identifikationsmidler og tillidstjenester, er formålet med denne forordning at:

a) fastlægge betingelserne for, hvordan medlemsstaterne anerkender elektroniske identifikationsmidler for fysiske og juridiske personer, der er omfattet af en anmeldt elektronisk identifikationsordning i en anden medlemsstat

b) fastlægge regler for tillidstjenester, navnlig for elektroniske transaktioner, og

c) opstille et retsgrundlag for elektroniske signaturer, elektroniske segl, elektroniske tidsstempler, elektroniske dokumenter, elektroniske registrerede leveringstjenester og certificeringstjenester for webstedsautentifikation.

Artikel 2

Anvendelsesområde

1. Denne forordning finder anvendelse på elektroniske identifikationsordninger, der er blevet anmeldt af en medlemsstat, samt på tillidstjenesteudbydere, der er hjemmehørende i Unionen.

2. Denne forordning finder ikke anvendelse på levering af tillidstjenester, der udelukkende anvendes i lukkede systemer i henhold til national ret eller aftaler mellem et defineret sæt deltagere.

3. Denne forordning påvirker ikke national ret eller EU-ret vedrørende kontrakters indgåelse og gyldighed eller andre retlige eller proceduremæssige forpligtelser, der vedrører formkrav.

Artikel 3

Definitioner

I denne forordning forstås ved:

1) »elektronisk identifikation«: det at bruge personidentifikationsdata i elektronisk form, der entydigt repræsenterer enten en fysisk eller juridisk person eller en fysisk person, der repræsenterer en juridisk person

2) »elektronisk identifikationsmiddel«: en materiel og/eller immateriel enhed, der indeholder personidentifikationsdata, og som bruges til autentifikation i forbindelse med en onlinetjeneste

3) »personidentifikationsdata«: et sæt data, der gør det muligt at fastslå identiteten på en fysisk eller juridisk person eller en fysisk person, der repræsenterer en juridisk person

4) »elektronisk identifikationsordning«: et system til elektronisk identifikation, under hvilket der udstedes elektroniske identifikationsmidler til fysiske eller juridiske eller fysiske personer, der repræsenterer juridiske personer

5) »autentifikation«: en elektronisk proces, der muliggør bekræftelse af den elektroniske identifikation af en fysisk eller juridisk person eller oprindelsen og integriteten af data i elektronisk form

6) »modtagerpart«: en fysisk eller juridisk person, der er afhængig af en elektronisk identifikations- eller tillidstjeneste

7) »offentlig myndighed«: en statslig, regional eller lokal myndighed, et offentligretligt organ eller en sammenslutning af en eller flere af disse myndigheder eller et eller flere af disse offentligretlige organer eller en privat enhed med mandat fra mindst en af disse myndigheder, organer eller sammenslutninger til at udbyde offentlige tjenester, når den optræder i henhold til et sådant mandat

8) »offentligretligt organ«: et organ som defineret i artikel 2, stk. 1, nr. 4), i Europa-Parlamentets og Rådets direktiv 2014/24/EU ([1])

9) »underskriver«: en fysisk person, der genererer en elektronisk signatur

10) »elektronisk signatur«: data i elektronisk form, der er vedhæftet eller logisk tilknyttet andre data i elektronisk form, og som anvendes af underskriveren til at skrive under med

11) »avanceret elektronisk signatur«: en elektronisk signatur, der opfylder kravene i artikel 26

12) »kvalificeret elektronisk signatur«: en avanceret elektronisk signatur, der er genereret af et kvalificeret elektronisk signaturgenereringssystem og baseret på et kvalificeret certifikat for elektroniske signaturer

13) »elektroniske signaturgenereringsdata«: entydige data, som anvendes af underskriveren til at generere en elektronisk signatur

14) »certifikat for elektronisk signatur«: en elektronisk attestering, som knytter elektroniske signaturvalideringsdata til en fysisk person og mindst bekræfter denne persons navn eller pseudonym

15) »kvalificeret certifikat for elektronisk signatur«: et certifikat for elektroniske signaturer, som er udstedt af en kvalificeret tillidstjenesteudbyder og opfylder kravene i bilag I

16) »tillidstjeneste«: en elektronisk tjeneste, der normalt udføres mod betaling, og som består af:

   a) generering, kontrol og validering af elektroniske signaturer, elektroniske segl eller elektroniske tidsstempler, elektroniske registrerede leveringstjenester og certifikater relateret til disse tjenester, eller

   b) generering, kontrol og validering af certifikater for webstedsautentifikation, eller

   c) bevaring af elektroniske signaturer, segl eller certifikater relateret til disse tjenester

17) »kvalificeret tillidstjeneste«: en tillidstjeneste, der opfylder de krav, der er fastsat i denne forordning

([1]) Europa-Parlamentets og Rådets direktiv 2014/24/EU af 26. februar 2014 om offentlige udbud og om ophævelse af direktiv 2004/18/EF (EUT L 94 af 28.3.2014, s. 65).

18) »overensstemmelsesvurderingsorgan«: et organ som defineret i artikel 2, nr. 13), i forordning (EF) nr. 765/2008, der er akkrediteret i overensstemmelse med nævnte forordning med kompetence til at udføre overensstemmelsesvurderinger af en kvalificeret tillidstjenesteudbyder og de kvalificerede tillidstjenester, den udbyder

19) »tillidstjenesteudbyder«: en fysisk eller juridisk person, der udbyder en eller flere tillidstjenester, som enten en kvalificeret eller ikkekvalificeret tillidstjenesteudbyder

20) »kvalificeret tillidstjenesteudbyder«: en tillidstjenesteudbyder, der udbyder en eller flere kvalificerede tillidstjenester og har fået tildelt status som kvalificeret tillidstjenesteudbyder af tilsynsorganet

21) »produkt«: hardware eller software eller relevante hardware- eller softwarekomponenter, som er beregnet til at blive brugt til levering af tillidstjenester

22) »elektronisk signaturgenereringssystem«: konfigureret software eller hardware, der bruges til at generere en elektronisk signatur

23) »kvalificeret elektronisk signaturgenereringssystem«: et elektronisk signaturgenereringssystem, der opfylder kravene i bilag II

24) »forseglende part«: en juridisk person, der genererer et elektronisk segl

25) »elektronisk segl«: data i elektronisk form, der er vedhæftet eller logisk tilknyttet andre data i elektronisk form, og som giver sikkerhed for disse tilknyttede datas oprindelse og integritet

26) »avanceret elektronisk segl«: et elektronisk segl, der opfylder kravene fastsat i artikel 36

27) »kvalificeret elektronisk segl«: et avanceret elektronisk segl, der er genereret af et kvalificeret elektronisk seglgenereringssystem, og som er baseret på et kvalificeret certifikat for elektroniske segl

28) »elektroniske seglgenereringsdata«: entydige data, som anvendes af den forseglende part til at generere et elektronisk segl

29) »certifikat for elektronisk segl«: en elektronisk attestering, som knytter elektroniske seglvalideringsdata til en fysisk person og bekræfter denne persons navn

30) »kvalificeret certifikat for elektronisk segl«: et certifikat for et elektronisk segl, som er udstedt af en kvalificeret tillidstjenesteudbyder og opfylder kravene i bilag III

31) »elektronisk seglgenereringssystem«: konfigureret software eller hardware, der bruges til at generere et elektronisk segl

32) »kvalificeret elektronisk seglgenereringssystem«: et elektronisk seglgenereringssystem, der med de fornødne ændringer opfylder kravene i bilag II

33) »elektronisk tidsstempel«: data i elektronisk form, der forbinder andre data i elektronisk form med et bestemt tidspunkt og udgør bevis for, at disse andre data eksisterede på det pågældende tidspunkt

34) »kvalificeret elektronisk tidsstempel«: et elektronisk tidsstempel, der opfylder kravene i artikel 42

35) »elektronisk dokument«: al form for indhold, der er lagret i elektronisk form, især som tekst eller lyd eller i visuel eller audiovisuel form

36) »elektronisk registreret leveringstjeneste«: en tjeneste, der gør det muligt at sende data mellem tredjeparter ad elektronisk vej og dokumenterer behandlingen af de sendte data, herunder leverer bevis for afsendelse og modtagelse af dataene, og som beskytter de sendte data mod tab, tyveri, beskadigelse og uautoriseret ændring

37) »kvalificeret elektronisk registreret leveringstjeneste«: en elektronisk registreret leveringstjeneste, der opfylder kravene i artikel 44

38) »certifikat for webstedsautentifikation«: en attestering, der gør det muligt at autentificere et websted og knytter webstedet til den fysiske eller juridiske person, som certifikatet er udstedt til

39) »kvalificeret certifikat for webstedsautentifikation«: et certifikat for webstedsautentifikation, der er udstedt af en kvalificeret tillidstjenesteudbyder og opfylder kravene i bilag IV

40) »valideringsdata«: data, der bruges til at validere en elektronisk signatur eller et elektronisk segl

41) »validering«: en fremgangsmåde til at kontrollere og bekræfte gyldigheden af en elektronisk signatur eller et elektronisk segl.

Artikel 4

Principper vedrørende det indre marked

1. Tillidstjenesteudbydere har ret til uden restriktioner at udbyde deres tjenester i en anden medlemsstat end den, hvor de er hjemmehørende, når tjenesterne udbydes med et formål, der er omfattet af denne forordning.

2. Der er fri bevægelighed på det indre marked for produkter og tillidstjenester, der overholder bestemmelserne i denne forordning.

Artikel 5

Databehandling og databeskyttelse

1. Behandling af personoplysninger skal udføres i overensstemmelse med direktiv 95/46/EF.

2. Uden at den retsvirkning, der tillægges pseudonymer i henhold til den nationale ret dermed foregribes, må anvendelsen af pseudonymer i elektroniske transaktioner ikke forbydes.

KAPITEL II

ELEKTRONISK IDENTIFIKATION

Artikel 6

Gensidig anerkendelse

1. Når der i henhold til national ret eller administrativ praksis kræves elektronisk identifikation ved hjælp af et elektronisk identifikationsmiddel og autentifikation som forudsætning for adgang til en onlinetjeneste, der udbydes af en offentlig myndighed i en medlemsstat, skal det elektroniske identifikationsmiddel, der er udstedt i en anden medlemsstat, anerkendes i den første medlemsstat med henblik på grænseoverskridende autentifikation af denne onlinetjeneste, forudsat at følgende betingelser er opfyldt:

a) det elektroniske identifikationsmiddel er udstedt under en elektronisk identifikationsordning, der er opført på den liste, som Kommissionen offentliggør i henhold til artikel 9

b) sikringsniveauet for det elektroniske identifikationsmiddel svarer til et sikringsniveau, der modsvarer eller er højere end det sikringsniveau, der kræves af den relevante offentlige myndighed for at få adgang til den pågældende onlinetjeneste i den første medlemsstat, forudsat at sikringsniveauet for det pågældende elektroniske identifikationsmiddel svarer til sikringsniveauet »betydelig« eller »høj«

c) den relevante offentlige myndighed anvender sikringsniveauet »betydelig« eller »høj« i forbindelse med adgang til den pågældende onlinetjeneste.

En sådan anerkendelse skal finde sted senest 12 måneder efter, at Kommissionen offentliggør den i første afsnit, litra a), omhandlede liste.

2. Et elektronisk identifikationsmiddel, der er udstedt under en elektronisk identifikationsordning, som er opført på den liste, som Kommissionen offentliggør i henhold til artikel 9, og som svarer til sikringsniveauet »lav«, kan anerkendes af offentlige myndigheder med henblik på grænseoverskridende autentifikation af disse myndigheders tjenester, der udbydes online.

Artikel 7

Antagelse af anmeldelser af elektroniske identifikationsordninger

En elektronisk identifikationsordning kan anmeldes i henhold til artikel 9, stk. 1, hvis alle nedenstående betingelser er opfyldt:

a) det elektroniske identifikationsmiddel under den elektroniske identifikationsordning er udstedt:

i) af den anmeldende medlemsstat

ii) i henhold til et mandat fra den anmeldende medlemsstat, eller

iii) uafhængigt af den anmeldende medlemsstat og anerkendt af den pågældende medlemsstat

b) det elektroniske identifikationsmiddel under den elektroniske identifikationsordning kan bruges til at få adgang til mindst en tjeneste, som udbydes af en offentlig myndighed, og som kræver elektronisk identifikation i den anmeldende medlemsstat

c) den elektroniske identifikationsordning og de elektroniske identifikationsmidler, der er udstedt i medfør heraf, opfylder kravene i mindst ét af de sikringsniveauer, der er fastsat i den gennemførelsesretsakt, som er omhandlet i artikel 8, stk. 3

d) den anmeldende medlemsstat sikrer, at de personidentifikationsdata, der entydigt repræsenterer den pågældende person, i overensstemmelse med de tekniske specifikationer, standarderne og procedurerne for det relevante sikringsniveau, der er anført i den gennemførelsesretsakt, som er omhandlet i artikel 8, stk. 3, er knyttet til den i artikel 3, nr. 1), omhandlede fysisk eller juridisk person på tidspunktet for udstedelsen af de elektroniske identifikationsmidler under denne ordning

e) den part, der udsteder det elektroniske identifikationsmiddel under denne ordning, sikrer, at det elektroniske identifikationsmiddel, der knyttes til den person, der er omhandlet i litra d) i nærværende artikel, er i overensstemmelse med de tekniske specifikationer, standarderne og procedurerne for det relevante sikringsniveau, der er fastsat i den gennemførelsesretsakt, som er omhandlet i artikel 8, stk. 3

f) den anmeldende medlemsstat sikrer, at der er onlineadgang til autentifikation, så enhver modtagerpart, der er hjemmehørende på en anden medlemsstats område, kan bekræfte de personidentifikationsdata, der er modtaget i elektronisk form.

For modtagerparter, der ikke er offentlige myndigheder, kan den anmeldende medlemsstat fastsætte betingelser for adgang til den pågældende autentifikation. Den grænseoverskridende autentifikation skal foretages gratis, når den gennemføres i forbindelse med en onlinetjeneste, der udbydes af en offentlig myndighed.

Medlemsstaterne må ikke pålægge modtagerparter, som vil gennemføre en sådan autentifikation, urimelige tekniske krav, når sådanne krav forhindrer eller i væsentligt omfang hindrer interoperabilitet mellem de anmeldte elektroniske identifikationsordninger

g) senest seks måneder forud for anmeldelsen i henhold til artikel 9, stk. 1, fremlægger den anmeldende medlemsstat på baggrund af forpligtelsen i artikel 12, stk. 5, en beskrivelse af ordningen for de andre medlemsstater i overensstemmelse med de proceduremæssige ordninger, der er fastsat ved de i artikel 12, stk. 7, omhandlede gennemførelsesretsakter

h) den elektroniske identifikationsordning opfylder de krav, der er fastsat i den i artikel 12, stk. 8, omhandlede gennemførelsesretsakt.

Artikel 8

Sikringsniveauer for elektroniske identifikationsordninger

1. En elektronisk identifikationsordning, der er anmeldt i henhold til artikel 9, stk. 1, skal angive sikringsniveauerne »lav«, »betydelig« og/eller »høj« for de elektroniske identifikationsmidler, der er udstedt under den pågældende ordning.

2. Sikringsniveauerne »lav«, »betydelig« og »høj« skal opfylde følgende kriterier:

a) sikringsniveauet »lav« henviser til et elektronisk identifikationsmiddel i en elektronisk identifikationsordning, der udviser en begrænset grad af tillid til en persons påståede identitet, og som er karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at mindske risikoen for misbrug eller ændring af identiteten

b) sikringsniveauet »betydelig« henviser til et elektronisk identifikationsmiddel i en elektronisk identifikationsordning, der udviser en middelstor grad af tillid til en persons påståede identitet, og som er karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at mindske risikoen for misbrug eller ændring af identiteten

c) sikringsniveauet »høj« henviser til et elektronisk identifikationsmiddel i en elektronisk identifikationsordning, der giver en højere grad af tillid til en persons påståede identitet end elektroniske identifikationsmidler med sikringsniveauet »betydelig«, og som er karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at mindske risikoen for misbrug eller ændring af identiteten.

3. Senest den 18. september 2015 fastsætter Kommissionen, idet der tages hensyn til relevante internationale standarder og med forbehold af stk. 2, ved hjælp af gennemførelsesretsakter de tekniske minimumsspecifikationer, minimumsstandarder, og procedurer, der henvises til i forbindelse med fastsættelse af sikringsniveauerne »lav«, »betydelig« og »høj« for de elektroniske identifikationsmidler, jf. stk. 1.

Disse tekniske minimumsspecifikationer, minimumsstandarder, og procedurer udarbejdes på grundlag af pålideligheden og kvaliteten af følgende elementer:

a) proceduren for godtgørelse og kontrol af identiteten på fysiske og juridiske personer, der ansøger om udstedelse af et elektronisk identifikationsmiddel

b) proceduren for udstedelse af det pågældende elektroniske identifikationsmiddel

c) autentifikationsmekanismen, hvorigennem den fysiske eller den juridiske person anvender det elektroniske identifikationsmiddel til at bekræfte vedkommendes identitet over for en modtagerpart

d) enheden, der udsteder det elektroniske identifikationsmiddel

e) ethvert andet organ, der er involveret i ansøgningsproceduren for udstedelse af det elektroniske identifikationsmiddel

f) de tekniske specifikationer og sikkerhedsspecifikationerne for det udstedte elektroniske identifikationsmiddel.

Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

Artikel 9

Anmeldelse

1. Den anmeldende medlemsstat meddeler Kommissionen nedenstående oplysninger og hurtigst muligt eventuelle senere ændringer heraf:

a) en beskrivelse af den elektroniske identifikationsordning, herunder dens sikringsniveau og udstederen eller udstederne af elektroniske identifikationsmidler under ordningen

b) den gældende tilsynsordning og oplysninger om erstatningsansvarsordningen med hensyn til følgende:

i) den part, der udsteder det elektroniske identifikationsmiddel, og

ii) den part, der udfører autentifikationsproceduren

c) oplysning om, hvilken eller hvilke myndigheder der er ansvarlige for den elektroniske identifikationsordning

d) oplysning om den eller de enheder, der forvalter registreringen af de entydige personidentifikationsdata

e) en beskrivelse af, hvordan kravene i gennemførelsesretsakterne, jf. artikel 12, stk. 8, opfyldes

f) en beskrivelse af den autentifikation, der er omhandlet i artikel 7, litra f)

g) nærmere bestemmelser om suspension eller spærring af den anmeldte elektroniske identifikationsordning eller autentifikationen eller de kompromitterede dele heraf.

2. Et år fra anvendelsesdatoen for gennemførelsesretsakterne, jf. artikel 8, stk. 3, og artikel 12, stk. 8, offentliggør Kommissionen i *Den Europæiske Unions Tidende* en liste over de elektroniske identifikationsordninger, der er anmeldt i henhold til stk. 1 i nærværende artikel, med grundlæggende oplysninger om ordningerne.

3. Modtager Kommissionen en anmeldelse efter udløbet af den periode, der er fastsat i stk. 2, offentliggør den i *Den Europæiske Unions Tidende* ændringerne af den i stk. 2 omhandlede liste inden for to måneder fra datoen for modtagelsen af denne anmeldelse.

4. En medlemsstat kan anmode Kommissionen om at fjerne en elektronisk identifikationsordning, der er anmeldt af den pågældende medlemsstat, fra den i stk. 2 omhandlede liste. Kommissionen offentliggør i *Den Europæiske Unions Tidende* de tilsvarende ændringer til listen inden for en måned fra datoen for medlemsstatens anmodning.

5. Kommissionen kan ved hjælp af gennemførelsesretsakter fastlægge vilkår, formater og procedurer for anmeldelser i medfør af stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

Artikel 10

Sikkerhedsbrud

1. Er enten en anmeldt elektronisk identifikationsordning i henhold til artikel 9, stk. 1, eller en autentifikation, jf. artikel 7, litra f), udsat for sikkerhedsbrud eller delvist kompromitteres på en måde, som har indvirkning på pålideligheden af den grænseoverskridende autentifikation i denne ordning, suspenderer eller tilbagekalder den anmeldende medlemsstat omgående den pågældende grænseoverskridende autentifikation eller de pågældende kompromitterede dele og underretter de øvrige medlemsstater og Kommissionen herom.

2. Når sikkerhedsbruddet eller kompromitteringen i stk. 1 afhjælpes, genopretter den anmeldende medlemsstat den grænseoverskridende autentifikation og underretter hurtigst muligt de øvrige medlemsstater og Kommissionen herom.

3. Afhjælpes sikkerhedsbruddet eller kompromitteringen som omhandlet i stk. 1 ikke inden for tre måneder efter suspensionen eller spærringen, underretter den anmeldende medlemsstat de øvrige medlemsstater og Kommissionen om tilbagekaldelsen af den elektroniske identifikationsordning.

Kommissionen offentliggør hurtigst muligt de nødvendige ændringer til listen, jf. artikel 9, stk. 2, i *Den Europæiske Unions Tidende*.

Artikel 11

Erstatningsansvar

1. Den anmeldende medlemsstat er erstatningsansvarlig for skader, der forsætligt eller uagtsomt påføres en fysisk eller juridisk person som følge af manglende overholdelse af forpligtelserne i henhold til artikel 7, litra d) og f), i forbindelse med en grænseoverskridende transaktion.

2. Den part, der udsteder det elektroniske identifikationsmiddel, er erstatningsansvarlig for skader, der forsætligt eller uagtsomt påføres en fysisk eller juridisk person som følge af manglende overholdelse af forpligtelsen i henhold til artikel 7, litra e), i forbindelse med en grænseoverskridende transaktion.

3. Den part, der udfører autentifikationsproceduren, er erstatningsansvarlig for skader, der forsætligt eller uagtsomt påføres en fysisk eller juridisk person som følge af manglende sikring af den korrekte udførelse af autentifikationen i henhold til artikel 7, litra f), i forbindelse med en grænseoverskridende transaktion.

4. Stk. 1, 2 og 3 anvendes i overensstemmelse med nationale regler om erstatningsansvar.

5. Stk. 1, 2 og 3 berører ikke det erstatningsansvar, der i henhold til national ret påhviler parterne i en transaktion, hvor der benyttes elektroniske identifikationsmidler, som er omfattet af den elektroniske identifikationsordning, der anmeldes i henhold til artikel 9, stk. 1.

Artikel 12

Samarbejde og interoperabilitet

1. De nationale elektroniske identifikationsordninger, der anmeldes i henhold til artikel 9, stk. 1, skal være interoperable.

2. Med henblik på stk. 1 indføres der en interoperabilitetsramme.

3. Interoperabilitetsrammen skal opfylde følgende kriterier:

a) den tager sigte på at være teknologineutral og forskelsbehandler ikke mellem specifikke nationale tekniske løsninger til elektronisk identifikation inden for en medlemsstat

b) den følger europæiske og internationale standarder, når det er muligt

c) den letter gennemførelsen af princippet om indbygget databeskyttelse (privacy by design), og

d) den sikrer, at personoplysninger behandles i overensstemmelse med direktiv 95/46/EF.

4. Interoperabilitetsrammen skal omfatte:

a) en henvisning til tekniske minimumskrav for sikringsniveauerne i artikel 8

b) en kortlægning af nationale sikringsniveauer for anmeldte elektroniske identifikationsordninger under sikringsniveauerne i artikel 8

c) en henvisning til tekniske minimumskrav for interoperabilitet

d) en henvisning til et minimum af personidentifikationsdata, der entydigt repræsenterer en fysisk eller juridisk person, og som stilles til rådighed fra elektroniske identifikationsordninger

e) forretningsorden

f) tvistbilæggelsesordninger, og

g) fælles operationelle sikkerhedsstandarder.

5. Medlemsstaterne skal samarbejde om følgende:

a) interoperabilitet mellem de elektroniske identifikationsordninger, der er anmeldt i henhold til artikel 9, stk. 1, og de elektroniske identifikationsordninger, som medlemsstaterne har til hensigt at anmelde, og

b) sikkerheden i de elektroniske identifikationsordninger.

6. Samarbejdet mellem medlemsstaterne omfatter:

a) udvekslingen af oplysninger, erfaring og god praksis med hensyn til elektroniske identifikationsordninger og navnlig tekniske krav til interoperabilitet og sikringsniveauer

b) udvekslingen af oplysninger, erfaring og god praksis med hensyn til arbejdet med sikringsniveauer i elektroniske identifikationsordninger i henhold til artikel 8

c) fagfællebedømmelse (peer review) af elektroniske identifikationsordninger, der henhører under denne forordning, og

d) undersøgelse af relevante udviklingstendenser i sektoren for elektronisk identifikation.

7. Senest den 18. marts 2015 fastlægger Kommissionen ved hjælp af gennemførelsesretsakter de fornødne proceduremæssige ordninger for at lette samarbejdet mellem medlemsstaterne, jf. stk. 5 og 6, med henblik på at fremme et højt niveau af tillid og sikkerhed, der står i et passende forhold til risikoen.

8. Senest den 18. september 2015 vedtager Kommissionen med forbehold af kriterierne i stk. 3 og under hensyn til resultaterne af samarbejdet mellem medlemsstaterne gennemførelsesretsakter om interoperabilitetsrammen som fastsat i stk. 4 med henblik på at fastsætte ensartede betingelser for gennemførelsen af kravet i stk. 1.

9. De i stk. 7 og 8 i nærværende artikel omhandlede gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

KAPITEL III

TILLIDSTJENESTER

AFDELING 1

Almindelige bestemmelser

Artikel 13

Erstatningsansvar og bevisbyrde

1. Uden at det berører stk. 2 er tillidstjenesteudbydere erstatningsansvarlige for skade, der forsætligt eller uagtsomt påføres en fysisk eller juridisk person som følge af manglende overholdelse af forpligtelserne i denne forordning.

Den fysiske eller juridiske person, der hævder at have lidt skade som omhandlet i første afsnit, bærer bevisbyrden for, at en ikkekvalificeret tillidstjenesteudbyder har handlet forsætligt eller uagtsomt.

En kvalificeret tillidstjenesteudbyder formodes at have handlet forsætligt eller uagtsomt, medmindre den pågældende kvalificerede tillidstjenesteudbyder beviser, at den i første afsnit omhandlede skade opstod uden forsæt eller uagtsomhed fra den pågældende kvalificerede tillidstjenesteudbyders side.

2. Når tillidstjenesteudbydere behørigt forudgående underretter deres kunder om begrænsningerne i forbindelse med anvendelsen af de tjenester, de udbyder, og når disse begrænsninger er identificerbare for tredjeparter, er tillidstjenesteudbydere ikke erstatningsansvarlige for skader, der påføres i forbindelse med anvendelse af tjenester, der går ud over de anførte begrænsninger.

3. Stk. 1 og 2 anvendes i overensstemmelse med nationale regler om erstatningsansvar.

Artikel 14

Internationale aspekter

1. Tillidstjenester der udbydes af tillidstjenesteudbydere, som er hjemmehørende i et tredjeland, anerkendes som retligt ligestillede med kvalificerede tillidstjenester, der udbydes af kvalificerede tillidstjenesteudbydere, der er hjemmehørende i Unionen, hvis de tillidstjenester, der har oprindelse i tredjelandet, anerkendes i henhold til en aftale, som er indgået mellem Unionen og det pågældende tredjeland eller en international organisation i overensstemmelse med artikel 218 i TEUF.

2. Aftaler som omhandlet i stk. 1 skal navnlig sikre, at:

a) tillidstjenesteudbyderne i det tredjeland eller de internationale organisationer, som aftalen indgås med, og de tillidstjenester, de udbyder, opfylder de krav, der gælder for kvalificerede tillidstjenesteudbydere, som er hjemmehørende i Unionen, og de kvalificerede tillidstjenester, de udbyder

b) de kvalificerede tillidstjenester, der udbydes af kvalificerede tillidstjenesteudbydere, som er hjemmehørende i Unionen, anerkendes som retligt ligestillede med tillidstjenester, der udbydes af tillidstjenesteudbydere i det tredjeland eller den internationale organisation, som aftalen indgås med.

Artikel 15

Tilgængelighed for personer med handicap

Når det er muligt, gøres tillidstjenester og slutbrugerprodukter, der bruges til levering af disse tjenester, tilgængelige for handicappede.

Artikel 16

Sanktioner

Medlemsstaterne fastsætter regler om sanktioner for overtrædelse af denne forordning. Sanktionerne skal være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

AFDELING 2

Tilsyn

Artikel 17

Tilsynsorganer

1. Hver medlemsstat udpeger et tilsynsorgan, der er hjemmehørende på dens område, eller, efter gensidig aftale med en anden medlemsstat, et tilsynsorgan, der er hjemmehørende i den pågældende anden medlemsstat. Dette organ er ansvarligt for tilsynsopgaver i den udpegende medlemsstat.

Tilsynsorganerne tillægges de nødvendige beføjelser og tilstrækkelige ressourcer til varetagelsen af deres opgaver.

2. Medlemsstaterne meddeler Kommissionen navn og adresse på de tilsynsorganer, de hver især har udpeget.

3. Tilsynsorganet har følgende rolle:

a) at føre tilsyn med kvalificerede tillidstjenesteudbydere, der er hjemmehørende på den udpegende medlemsstats område, for ved hjælp af forudgående og efterfølgende tilsynsvirksomhed at sikre, at disse kvalificerede tillidstjenesteudbydere og de kvalificerede tillidstjenester, de udbyder, opfylder kravene i denne forordning

b) om nødvendigt at gribe ind over for ikkekvalificerede tillidstjenesteudbydere, der er hjemmehørende på den udpegende medlemsstats område ved hjælp af efterfølgende tilsynsvirksomhed, når det underrettes om, at disse ikkekvalificerede tillidstjenesteudbydere eller de tillidstjenester, de udbyder, angiveligt ikke opfylder kravene i denne forordning.

4. Med henblik på stk. 3 og med forbehold af de deri fastsatte begrænsninger omfatter tilsynsorganets opgaver navnlig:

a) at samarbejde med andre tilsynsorganer og yde dem bistand i overensstemmelse med artikel 18

b) at analysere de overensstemmelsesvurderingsrapporter, der er omhandlet i artikel 20, stk. 1, og artikel 21, stk. 1

c) at underrette andre tilsynsorganer og offentligheden om brud på sikkerheden eller tab af integritet i overensstemmelse med artikel 19, stk. 2

d) at aflægge rapport til Kommissionen om sin primære virksomhed i overensstemmelse med stk. 6 i nærværende artikel

e) at foretage kontrolundersøgelser eller anmode et overensstemmelsesvurderingsorgan om at udføre en overensstemmelsesvurdering af de kvalificerede tillidstjenesteudbydere i overensstemmelse med artikel 20, stk. 2

f) at samarbejde med databeskyttelsesmyndighederne, navnlig ved hurtigst muligt at underrette dem om resultaterne af kontrolundersøgelser af kvalificerede tillidstjenesteudbydere, hvis der er mistanke om overtrædelse af reglerne om beskyttelse af personoplysninger

g) at tildele kvalificerede tillidstjenesteudbydere og de tjenester, de udbyder, status som kvalificeret og at trække denne status tilbage i overensstemmelse med artikel 20 og 21

h) at underrette det organ, der er ansvarligt for den nationale positivliste, der er omhandlet i artikel 22, stk. 3, om sine afgørelser om tildeling eller tilbagetrækning af status som kvalificeret, medmindre dette organ også er tilsynsorganet

i) at kontrollere, at der findes bestemmelser om planer for virksomhedsafbrydelse, og at de anvendes korrekt, i tilfælde hvor den kvalificerede tillidstjenesteudbyder afbryder sin virksomhed, herunder hvordan oplysninger forbliver tilgængelige i overensstemmelse med artikel 24, stk. 2, litra h)

j) at pålægge tillidstjenesteudbydere at afhjælpe mangler i opfyldelsen af de krav, der er fastsat i denne forordning.

5. Medlemsstaterne kan kræve, at tilsynsorganet opretter, vedligeholder og ajourfører en tillidsinfrastruktur i overensstemmelse med betingelserne i national ret.

6. Senest den 31. marts hvert år forelægger tilsynsorganerne Kommissionen en rapport om det foregående kalenderårs primære tilsynsvirksomhed sammen med en sammenfatning af de indberetninger af brud på sikkerheden, som er modtaget fra tillidstjenesteudbydere i overensstemmelse med artikel 19, stk. 2.

7. Kommissionen gør den i stk. 6 omhandlede årlige rapport tilgængelig for medlemsstaterne.

8. Kommissionen kan ved hjælp af gennemførelsesretsakter fastlægge formater og procedurer for rapporteringen i medfør af stk. 6. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

Artikel 18

Gensidig bistand

1. Tilsynsorganerne skal samarbejde med henblik på at udveksle god praksis.

Et tilsynsorgan skal efter modtagelsen af en begrundet anmodning fra et andet tilsynsorgan yde det pågældende organ bistand, således at tilsynsorganernes arbejde kan udføres på en ensartet måde. Den gensidige bistand kan navnlig omfatte anmodninger om oplysninger og tilsynsforanstaltninger, f.eks. anmodninger om at foretage inspektioner i forbindelse med de overensstemmelsesvurderingsrapporter, der er omhandlet i artikel 20 og 21.

2. Et tilsynsorgan, der modtager en anmodning om bistand, kan afvise denne anmodning med en af følgende begrundelser:

a) tilsynsorganet er ikke kompetent til at yde den bistand, der anmodes om

b) anmodningen om bistand står ikke i rimeligt forhold til tilsynsorganets tilsynsvirksomhed udført i overensstemmelse med artikel 17

c) det ville være uforeneligt med denne forordning at yde den bistand, der anmodes om.

3. Når det er hensigtsmæssigt, kan medlemsstaterne tillade, at deres respektive tilsynsorganer i fællesskab gennemfører undersøgelser, hvor personale fra andre medlemsstaters tilsynsorganer deltager. Reglerne for og fremgangsmåden ved sådanne fælles aktioner skal aftales og fastlægges af de berørte medlemsstater i overensstemmelse med deres nationale ret.

Artikel 19

Sikkerhedskrav til tillidstjenesteudbydere

1. Kvalificerede og ikkekvalificerede tillidstjenesteudbydere skal træffe passende tekniske og organisatoriske foranstaltninger til at styre de sikkerhedsmæssige risici i forbindelse med de tillidstjenester, de udbyder. Under hensyn til den seneste teknologiske udvikling skal disse foranstaltninger garantere et sikkerhedsniveau, der svarer til risikoens omfang. Tillidstjenesteudbyderne bør navnlig tage skridt til at forhindre og minimere virkningen af sikkerhedsrelaterede hændelser og underrette de berørte parter om de negative virkninger af sådanne hændelser.

2. De kvalificerede og ikkekvalificerede tillidstjenesteudbydere, der konstaterer et brud på sikkerheden eller tab af integritet, som har en væsentlig indvirkning på den udbudte tillidstjeneste eller de berørte personoplysninger, skal hurtigst muligt og under alle omstændigheder inden for 24 timer efter at være blevet opmærksomme på forholdet underrette tilsynsorganet, og eventuelt andre relevante organer som f.eks. det kompetente nationale organ for informationssikkerhed eller databeskyttelsesmyndigheden.

Når det er sandsynligt, at et brud på sikkerheden eller tab af integritet vil krænke den fysiske eller juridiske person, som har modtaget tillidstjenesten, skal tillidstjenesteudbyderen også hurtigst muligt underrette den fysiske eller juridiske person om bruddet på sikkerheden eller tab af integritet.

Hvor det er relevant, og navnlig hvis et brud på sikkerheden eller tab af integritet berører to eller flere medlemsstater, skal det underrettede tilsynsorgan informere tilsynsorganerne i andre berørte medlemsstater og ENISA.

Det underrettede tilsynsorgan skal også informere offentligheden eller kræve, at tillidstjenesteudbyderen gør det, hvis det fastslår, at det er i offentlighedens interesse, at et brud på sikkerheden eller tab af integritet offentliggøres.

3. Tilsynsorganet forelægger en gang om året ENISA en sammenfattende rapport om de indberetninger af brud på sikkerheden eller tab af integritet, som det har modtaget fra tillidstjenesteudbyderne.

4. Kommissionen kan ved gennemførelsesretsakter:

a) yderligere specificere de i stk. 1 omhandlede foranstaltninger, og

b) vedtage formater og procedurer, herunder tidsfrister, for gennemførelsen af stk. 2.

Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

AFDELING 3

Kvalificerede tillidstjenesteydelser

Artikel 20

Tilsyn med kvalificerede tillidstjenesteudbydere

1. Kvalificerede tillidstjenesteudbydere skal kontrolleres af et overensstemmelsesvurderingsorgan for egen regning mindst hver 24. måned. Formålet med kontrollen er at bekræfte, at de kvalificerede tillidstjenesteudbydere og de kvalificerede tillidstjenester, som de udbyder, opfylder de krav, der er fastsat i denne forordning. De kvalificerede tillidstjenesteudbydere skal forelægge den resulterende overensstemmelsesvurderingsrapport for tilsynsorganet inden for en periode på tre arbejdsdage efter modtagelsen heraf.

2. Uden at dette berører stk. 1, kan tilsynsorganet til enhver tid foretage kontrol hos eller anmode et overensstemmelsesvurderingsorgan om at udføre en overensstemmelsesvurdering af de kvalificerede tillidstjenesteudbydere for disses tillidstjenesteudbyderes regning for at bekræfte, at de og deres kvalificerede tillidstjenester opfylder de krav, der er fastsat i denne forordning. Ved mistanke om overtrædelse af reglerne om beskyttelse af personoplysninger skal tilsynsorganet underrette databeskyttelsesmyndighederne om resultaterne af deres kontrolundersøgelser.

3. Kræver tilsynsorganet, at den kvalificerede tillidstjenesteudbyder afhjælper enhver forsømmelse af at opfylde kravene i denne forordning, og hvis tjenesteudbyderen ikke handler i overensstemmelse hermed og eventuelt inden for en af tilsynsorganet fastsat frist, kan tilsynsorganet under særlig hensyntagen til den omtalte mangels omfang, varighed og konsekvenser tilbagetrække den pågældende tjenesteudbyders eller den pågældende tjenestes status som kvalificeret og informere det organ, der er omhandlet i artikel 22, stk. 3, med henblik på at føre positivlisten i artikel 22, stk. 1, ajour. Tilsynsorganet underretter den kvalificerede tillidstjenesteudbyder om tilbagetrækningen af vedkommendes eller af den pågældende kvalificerede tjenestes status som kvalificeret.

4. Kommissionen kan ved hjælp af gennemførelsesretsakter opstille referencenumre på følgende standarder:

a) akkreditering af overensstemmelsesvurderingsorganerne og for overensstemmelsesvurderingsrapporten, jf. stk. 1

b) revisionsregler, i henhold til hvilke overensstemmelsesvurderingsorganer udfører deres overensstemmelsesvurdering af de kvalificerede tillidstjenesteudbydere, jf. stk. 1.

Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

Artikel 21

Iværksættelse af en kvalificeret tillidstjeneste

1. Ønsker en tillidstjenesteudbyder, der ikke har status som kvalificeret, at udbyde kvalificerede tillidstjenester, skal tjenesteudbyderen anmelde sin hensigt til tilsynsorganet og indsende en overensstemmelsesvurderingsrapport udstedt af et overensstemmelsesvurderingsorgan.

2. Tilsynsorganet kontrollerer, om tillidstjenesteudbyderen og de tillidstjenester, som vedkommende udbyder, opfylder de i denne forordning fastsatte krav, og navnlig kravene til kvalificerede tillidstjenesteudbydere og disses kvalificerede tillidstjenester.

Konkluderer tilsynsorganet, at tillidstjenesteudbyderen og de tillidstjenester, som vedkommende udbyder, overholder de i første afsnit omhandlede krav, tildeler tilsynsorganet tillidstjenesteudbyderen og de tillidstjenester, som vedkommende udbyder, status som kvalificeret og underretter senest tre måneder efter anmeldelsen, jf. stk. 1 i nærværende artikel, det organ, der er omhandlet i artikel 22, stk. 3, med henblik på at føre positivlisterne i artikel 22, stk. 1, ajour.

Er kontrollen ikke afsluttet inden tre måneder efter anmeldelsen, underretter tilsynsorganet tillidstjenesteudbyderen herom og forklarer årsagerne til forsinkelsen samt oplyser, hvornår kontrollen skal være afsluttet.

3. Kvalificerede tillidstjenesteudbydere kan begynde at udbyde den kvalificerede tillidstjeneste, når den kvalificerede status er indført på de i artikel 22, stk. 1, omhandlede positivlister.

4. Kommissionen kan ved hjælp af gennemførelsesretsakter fastlægge formater og procedurer med henblik på stk. 1 og 2. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

Artikel 22

Positivlister

1. Hver medlemsstat opretter, ajourfører og offentliggør positivlister herunder oplysninger om de kvalificerede tillidstjenesteudbydere, som den har ansvaret for, samt oplysninger om deres kvalificerede tillidstjenester.

2. Medlemsstaterne opretter, ajourfører og offentliggør under sikre forhold de elektronisk underskrevne eller forseglede positivlister, jf. stk. 1, i en form, der egner sig til automatiseret behandling.

3. Medlemsstaterne meddeler hurtigst muligt Kommissionen, hvilket organ der er ansvarligt for at oprette, ajourføre og offentliggøre de nationale positivlister, og hvor disse lister offentliggøres, og sender Kommissionen de certifikater, der er anvendt til underskrift eller forsegling af positivlisterne, og eventuelle ændringer heraf.

4. Kommissionen stiller de oplysninger, der er omhandlet i stk. 3, til rådighed for offentligheden via en sikker kommunikationsforbindelse og i en elektronisk underskrevet eller forseglet form, der egner sig til automatiseret behandling.

5. Senest den 18. september 2015 præciserer Kommissionen ved hjælp af gennemførelsesretsakter de oplysninger, der er anført i stk. 1, og fastlægger tekniske specifikationer og formater for positivlister med henblik på gennemførelsen af stk. 1-4. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

Artikel 23

EU-tillidsmærket for kvalificerede tillidstjenester

1. Efter at status som kvalificeret tillidstjenesteudbyder, jf. artikel 21, stk. 2, andet afsnit, er blevet angivet på den i artikel 22, stk. 1, omhandlede positivliste, kan kvalificerede tillidstjenesteudbydere anvende EU-tillidsmærket for på en enkel, genkendelig og klar måde at angive, hvilke kvalificerede tillidstjenester de udbyder.

2. Når EU-tillidsmærket anvendes for de i stk. 1 omhandlede kvalificerede tillidstjenester, skal de kvalificerede tillidstjenesteudbydere sikre, at der på deres websted findes et link til den relevante positivliste.

3. Senest den 1. juli 2015 fastlægger Kommissionen ved hjælp af gennemførelsesretsakter specifikationer med hensyn til formen og navnlig præsentationsformen, sammensætningen, størrelsen og udformningen af EU-tillidsmærket for kvalificerede tillidstjenester. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

Artikel 24

Krav til kvalificerede tillidstjenesteudbydere

1. Når en kvalificeret tillidstjenesteudbyder udsteder et kvalificeret certifikat for en tillidstjeneste, skal vedkommende med hensigtsmæssige midler og i overensstemmelse med national ret kontrollere identiteten og eventuelt særlige kendetegn ved den fysiske eller juridiske person, som det kvalificerede certifikat udstedes til.

Oplysningerne i første afsnit kontrolleres af den kvalificerede tillidstjenesteudbyder enten direkte eller via en tredjemand i overensstemmelse med national ret:

a) ved fysisk tilstedeværelse af den fysiske person eller den bemyndigede repræsentant for den juridiske person, eller

b) uden fysisk tilstedeværelse ved hjælp af elektroniske identifikationsmidler, hvortil der forud for udstedelsen af et kvalificeret certifikat var sikret en fysisk tilstedeværelse af den fysiske person eller af en bemyndiget repræsentant for den juridiske person, og som lever op til kravene i artikel 8 med hensyn til sikringsniveauet »betydelig« eller »høj«, eller

c) ved hjælp af et certifikat af en kvalificeret elektronisk signatur eller af et kvalificeret elektronisk segl udstedt i overensstemmelse med litra a) eller b), eller

d) ved hjælp af andre identifikationsmetoder anerkendt på nationalt plan, som giver en sikkerhed, der for så vidt angår pålidelighed svarer til fysisk tilstedeværelse. Den tilsvarende sikkerhed skal bekræftes af et overensstemmelsesvurderingsorgan.

2. En kvalificeret tillidstjenesteudbyder, der udbyder kvalificerede tillidstjenester, skal:

a) informere tilsynsorganet om ændringer i udbuddet af dennes kvalificerede tillidstjenester og om dennes hensigt om at ophøre med denne virksomhed

b) beskæftige personale, og eventuelt underleverandører, der har den nødvendige ekspertviden og troværdighed og de nødvendige erfaringer, og kvalifikationer, og som har fået tilstrækkelig uddannelse i reglerne for sikkerhed og beskyttelse af personoplysninger og skal anvende administrative og ledelsesmæssige procedurer i overensstemmelse med europæiske eller internationale standarder

c) i forbindelse med erstatningsansvaret for skader, have tilstrækkelige økonomiske ressourcer til rådighed, jf. artikel 13, og/eller anskaffe en passende ansvarsforsikring i overensstemmelse med national ret

d) på en klar og let forståelig måde underrette de personer, der ønsker at gøre brug af en kvalificeret tillidstjeneste, om de nøjagtige vilkår for brugen af denne tjeneste, herunder eventuelle begrænsninger i brugen heraf, inden de indgår i et kontraktforhold

e) anvende pålidelige systemer og produkter, som er beskyttet mod ændringer, og sikre den tekniske sikkerhed og pålidelighed i de processer, som disse systemer og produkter understøtter

f) benytte pålidelige systemer til opbevaring af de data, den kvalificerede tillidstjenesteudbyder modtager, i kontrollerbar form, således at

i) de kun er offentligt tilgængelige i de tilfælde, hvor den person, som dataene vedrører, har givet sit samtykke

ii) kun bemyndigede personer kan foretage tilføjelser til og ændringer af de opbevarede data

iii) dataenes ægthed kan kontrolleres

g) træffe passende foranstaltninger imod forfalskning og tyveri af data

h) i en rimelig periode registrere alle relevante oplysninger om de data, den kvalificerede tillidstjenesteudbyder har udstedt og modtaget, og sørge for, at de er tilgængelige, herunder efter at den kvalificerede tillidstjenesteudbyder har indstillet sin virksomhed, navnlig for at kunne fremlægge bevis i retssager og for at garantere tjenestens kontinuitet. Denne registrering kan ske elektronisk

i) have en ajourført plan i tilfælde af virksomhedsafbrydelse for at sikre tjenestens kontinuitet i overensstemmelse med de bestemmelser, som tilsynsorganer kontrollerer i medfør af artikel 17, stk. 4, litra i)

j) sikre, at personoplysninger behandles lovligt i overensstemmelse med direktiv 95/46/EF

k) oprette og ajourføre en certifikatdatabase, når den kvalificerede tillidstjenesteudbyder udsteder kvalificerede certifikater.

3. Vælger en kvalificeret tillidstjenesteudbyder, der udsteder kvalificerede certifikater, at spærre et certifikat, skal denne registrere en sådan spærring i sin certifikatdatabase og offentliggøre spærringen af certifikatet i god tid, og under alle omstændigheder inden for 24 timer efter modtagelsen af anmodningen. Spærringen træder i kraft straks efter offentliggørelsen.

4. Med hensyn til stk. 3 skal kvalificerede tillidstjenesteudbydere, der udsteder kvalificerede certifikater, stille oplysninger om certifikaternes gyldighed eller spærring til rådighed for alle modtagerparter. Disse oplysninger skal som minimum for et certifikat ad gangen være automatisk og gratis tilgængelige til enhver tid og ud over gyldighedsperioden på pålidelig og effektiv vis.

5. Kommissionen kan ved hjælp af gennemførelsesretsakter opstille referencenumre på standarder for pålidelige systemer og produkter, som opfylder kravene i stk. 2, litra e) og f), i nærværende artikel. Pålidelige systemer og produkter, der opfylder disse standarder, formodes at overholde kravene i nærværende artikel. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

AFDELING 4

Elektroniske signaturer

Artikel 25

Retsvirkninger af elektroniske signaturer

1. En elektronisk signatur må ikke nægtes retsvirkning og anerkendelse som bevis under retssager, alene af den grund at den er i elektronisk form, eller at den ikke opfylder kravene til kvalificerede elektroniske signaturer.

2. En kvalificeret elektronisk signatur har samme retsvirkning som en håndskreven underskrift.

3. En kvalificeret elektronisk signatur, som er baseret på et kvalificeret certifikat, der er udstedt i en medlemsstat, anerkendes som en kvalificeret elektronisk signatur i alle andre medlemsstater.

Artikel 26

Kravene til avancerede elektroniske signaturer

En avanceret elektronisk signatur skal opfylde følgende krav:

a) den er entydigt knyttet til underskriveren

b) den kan identificere underskriveren

c) den genereres ved hjælp af elektroniske signaturgenereringsdata, som underskriveren med en høj grad af tillid kan anvende og har fuld kontrol med, og

d) den er knyttet til de data, som er underskrevet med den, på en sådan måde, at en hvilken som helst senere ændring af disse data kan opdages.

Artikel 27

Elektroniske signaturer i offentlige tjenester

1. Kræver en medlemsstat en avanceret elektronisk signatur for at anvende en onlinetjeneste, der udbydes af eller på vegne af en offentlig myndighed, skal den pågældende medlemsstat anerkende avancerede elektroniske signaturer, avancerede elektroniske signaturer, som er baseret på et kvalificeret certifikat for elektroniske signaturer, og kvalificerede elektroniske signaturer som minimum i de formater eller ved anvendelse af de metoder, der er defineret i de i stk. 5 omhandlede gennemførelsesretsakter.

2. Kræver en medlemsstat en avanceret elektronisk signatur, som er baseret på et kvalificeret certifikat, for at anvende en onlinetjeneste, der udbydes af eller på vegne af en offentlig myndighed, skal den pågældende medlemsstat anerkende avancerede elektroniske signaturer, som er baseret på et kvalificeret certifikat, og kvalificerede elektroniske signaturer som minimum i de formater eller ved anvendelse af de metoder, der er defineret i de i stk. 5 omhandlede gennemførelsesretsakter.

3. I forbindelse med grænseoverskridende anvendelse af en onlinetjeneste, der udbydes af en offentlig myndighed, må medlemsstaterne ikke kræve en elektronisk signatur med et højere sikkerhedsniveau end det, der er forbundet med den kvalificerede elektroniske signatur.

4. Kommissionen kan ved hjælp af gennemførelsesretsakter opstille referencenumre på standarder for avancerede elektroniske signaturer. En avanceret elektronisk signatur, der opfylder disse standarder, formodes at overholde de krav til elektroniske signaturer, der er fastlagt i denne artikels stk. 1 og 2, og i artikel 26. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

5. Senest den 18. september 2015 og under hensyn til eksisterende praksis, standarder og EU-retsakter definerer Kommissionen ved hjælp af gennemførelsesretsakter referenceformater for avancerede elektroniske signaturer eller referencemetoder, når der anvendes alternative formater. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

Artikel 28

Kvalificerede certifikater for elektroniske signaturer

1. Kvalificerede certifikater for elektroniske signaturer skal opfylde kravene i bilag I.

2. Kvalificerede certifikater for elektroniske signaturer må ikke være omfattet af ufravigelige krav, der går videre end kravene i bilag I.

3. Kvalificerede certifikater for elektroniske signaturer kan omfatte ikkeobligatoriske supplerende særlige kendetegn. Disse kendetegn må ikke påvirke interoperabiliteten mellem og anerkendelsen af kvalificerede elektroniske signaturer.

4. Såfremt et kvalificeret certifikat for elektroniske signaturer er blevet spærret efter den første aktivering, mister det sin gyldighed fra tidspunktet for spærringen, og dets status kan under ingen omstændigheder genetableres.

5. Medlemsstaterne kan fastsætte nationale regler for en midlertidig suspension af et kvalificeret certifikat for elektroniske signaturer på følgende betingelser:

a) hvis et kvalificeret certifikat for elektroniske signaturer er blevet suspenderet midlertidigt, mister det sin gyldighed i suspensionsperioden

b) suspensionsperioden angives klart i certifikatdatabasen, og suspensionsstatus gøres synlig i suspensionsperioden af den tjeneste, der formidler oplysninger om status for certifikatet.

6. Kommissionen kan ved hjælp af gennemførelsesretsakter opstille referencenumre på standarder for kvalificerede certifikater for elektroniske signaturer. Et kvalificeret certifikat for elektroniske signaturer, der opfylder disse standarder, formodes at overholde kravene i bilag I. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

Artikel 29

Krav til kvalificerede elektroniske signaturgenereringssystemer

1. Kvalificerede elektroniske signaturgenereringssystemer skal opfylde kravene i bilag II.

2. Kommissionen kan ved hjælp af gennemførelsesretsakter opstille referencenumre på standarder for kvalificerede elektroniske signaturgenereringssystemer. Et kvalificeret elektronisk signaturgenereringssystem, der opfylder disse standarder, formodes at overholde kravene i bilag II. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

Artikel 30

Certificering af kvalificerede elektroniske signaturgenereringssystemer

1. Egnede offentlige eller private organer, der udpeges af medlemsstaterne, skal certificere overensstemmelsen mellem de kvalificerede elektroniske signaturgenereringssystemer og de i bilag II fastsatte krav.

2. Medlemsstaterne meddeler Kommissionen navn og adresse på de i stk. 1 omhandlede offentlige eller private organer. Kommissionen stiller disse oplysninger til rådighed for medlemsstaterne.

3. Certificeringen i stk. 1 baseres på en af følgende processer:

a) en sikkerhedsevalueringsproces, som gennemføres i overensstemmelse med en af de standarder for sikkerhedsvurdering af informationsteknologiprodukter, der er opført på den liste, der er udarbejdet i overensstemmelse med andet afsnit, eller

b) en anden proces end den i litra a) omhandlede, såfremt den anvender sammenlignelige sikkerhedsniveauer og såfremt det i stk. 1 omhandlede offentlige eller private organ meddeler denne proces til Kommissionen. Den pågældende proces kan kun anvendes, hvis de standarder, der er omhandlet i litra a), ikke findes, eller hvis en sikkerhedsevalueringsproces som omhandlet i litra a) ikke er afsluttet.

Kommissionen udarbejder ved hjælp af gennemførelsesretsakter en liste over standarder for sikkerhedsvurderingen af de informationsteknologiprodukter, der er omhandlet i litra a). Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

4. Kommissionen tillægges beføjelse til at vedtage delegerede retsakter i overensstemmelse med artikel 47 vedrørende fastsættelsen af de særlige kriterier, som de i stk. 1 i nærværende artikel omhandlede udpegede organer skal opfylde.

Artikel 31

Offentliggørelse af en liste over certificerede kvalificerede elektroniske signaturgenereringssystemer

1. Medlemsstaterne forelægger uden unødig forsinkelse og senest en måned efter, at certificeringen er blevet afsluttet, Kommissionen oplysninger om de kvalificerede elektroniske signaturgenereringssystemer, der er certificeret af de organer, der er omhandlet i artikel 30, stk. 1. De underretter også hurtigst muligt og senest en måned efter, at certificeringen er blevet annulleret, Kommissionen om kvalificerede elektroniske signaturgenereringssystemer, der ikke længere er certificeret.

2. På grundlag af de modtagne oplysninger opstiller Kommissionen en liste over certificerede kvalificerede elektroniske signaturgenereringssystemer, som den offentliggør og fører ajour.

3. Kommissionen kan ved hjælp af gennemførelsesretsakter fastlægge formater og procedurer for gennemførelsen af stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

Artikel 32

Krav til validering af kvalificerede elektroniske signaturer

1. Processen for validering af en kvalificeret elektronisk signatur skal bekræfte gyldigheden af en kvalificeret elektronisk signatur, såfremt:

a) det certifikat, der støtter signaturen, på underskriftstidspunktet var et kvalificeret certifikat for elektronisk signatur, der var i overensstemmelse bilag I

b) det kvalificerede certifikat var udstedt af en kvalificeret tillidstjenesteudbyder og var gyldigt på underskriftstidspunktet

c) signaturvalideringsdataene stemmer overens med de data, der leveres til modtagerparten

d) det entydige sæt data, der repræsenterer underskriveren i certifikatet, leveres korrekt til modtagerparten

e) en eventuel anvendelse af et pseudonym fremgår klart for modtagerparten, såfremt der på underskriftstidspunktet blev anvendt et pseudonym

f) den elektroniske signatur er genereret af et kvalificeret elektronisk signaturgenereringssystem

g) de underskrevne datas integritet ikke er bragt i fare

h) kravene i artikel 26 var opfyldt på underskriftstidspunktet.

2. Det system, der anvendes til validering af den kvalificerede elektroniske signatur, skal levere det korrekte resultat af valideringsprocessen til modtagerparten og gøre det muligt for vedkommende at opdage eventuelle sikkerhedsproblemer.

3. Kommissionen kan ved hjælp af gennemførelsesretsakter opstille referencenumre på standarder for validering af kvalificerede elektroniske signaturer. En validering af kvalificerede elektroniske signaturer, der opfylder disse standarder, formodes at overholde kravene i stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

Artikel 33

Kvalificeret valideringstjeneste for kvalificerede elektroniske signaturer

1. En kvalificeret valideringstjeneste for kvalificerede elektroniske signaturer må kun stilles til rådighed af en kvalificeret tillidstjenesteudbyder, der

a) udfører validering i overensstemmelse med artikel 32, stk. 1, og

b) gør det muligt for modtagerparter automatisk at modtage resultatet af valideringsprocessen på pålidelig og effektiv vis, hvor resultatet er forsynet med valideringstjenesteudbyderens avancerede elektroniske signatur eller avancerede elektroniske segl.

2. Kommissionen kan ved hjælp af gennemførelsesretsakter opstille referencenumre på standarder for kvalificerede valideringstjenester, jf. stk. 1. En valideringstjeneste for en kvalificeret elektronisk signatur, der opfylder disse standarder, formodes at overholde kravene i stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

Artikel 34

Kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer

1. En kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer må kun stilles til rådighed af en kvalificeret tillidstjenesteudbyder, der anvender procedurer og teknologier, der gør det muligt at forlænge pålideligheden af den kvalificerede elektroniske signatur ud over den teknologiske gyldighedsperiode.

2. Kommissionen kan ved hjælp af gennemførelsesretsakter opstille referencenumre på standarder for kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer. En kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer, der opfylder disse standarder, formodes at overholde kravene i stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

AFDELING 5

Elektroniske segl

Artikel 35

Retsvirkninger af elektroniske segl

1. Et elektronisk segl må ikke nægtes retsvirkning og anerkendelse som bevis under retssager, alene af den grund at det er i elektronisk form, eller at det ikke opfylder kravene til kvalificerede elektroniske segl.

2. For et kvalificeret elektronisk segl, gælder der en formodning for integriteten af de data og nøjagtigheden af oprindelsen af de data, som det kvalificerede elektroniske segl er knyttet til.

3. Et kvalificeret elektronisk segl, som er baseret på et kvalificeret certifikat og udstedt i en medlemsstat, anerkendes som et kvalificeret elektronisk segl i alle andre medlemsstater.

Artikel 36

Krav til avancerede elektroniske segl

Et avanceret elektronisk segl skal opfylde følgende krav:

a) det er entydigt knyttet til den forseglende part

b) det kan identificere den forseglende part

c) det genereres ved hjælp af elektroniske seglgenereringsdata, som den forseglende part med en høj grad af tillid og fuld kontrol kan anvende til at generere elektroniske segl, og

d) det er knyttet til de data, som det vedrører, på en sådan måde, at en hvilken som helst senere ændring af disse data kan opdages.

Artikel 37

Elektroniske segl i offentlige tjenester

1. Kræver en medlemsstat et avanceret elektronisk segl som forudsætning for adgang til en onlinetjeneste, der udbydes af eller på vegne af en offentlig myndighed, skal den pågældende medlemsstat anerkende avancerede elektroniske segl, avancerede elektroniske segl, som er baseret på et kvalificeret certifikat for elektroniske segl, og kvalificerede elektroniske segl som minimum i de formater eller ved anvendelse af de metoder, der er defineret i de i stk. 5 omhandlede gennemførelsesretsakter.

2. Kræver en medlemsstat et avanceret elektronisk segl, som er baseret på et kvalificeret certifikat som forudsætning for adgang til en onlinetjeneste, der udbydes af eller på vegne af en offentlig myndighed, skal den pågældende medlemsstat anerkende avancerede elektroniske segl, som er baserede på et kvalificeret certifikat, og kvalificerede elektroniske segl som minimum i de formater eller ved anvendelse af de metoder, der er defineret i de i stk. 5 omhandlede gennemførelsesretsakter.

3. I forbindelse med grænseoverskridende anvendelse af en onlinetjeneste, der udbydes af en offentlig myndighed, må medlemsstaterne ikke kræve et elektronisk segl på et højere sikkerhedsniveau end det, der er forbundet med et kvalificeret elektronisk segl.

4. Kommissionen kan ved hjælp af gennemførelsesretsakter opstille referencenumre på standarder for avancerede elektroniske segl. Et avanceret elektronisk segl, der opfylder disse standarder, formodes at overholde de krav til elektroniske segl, der er fastlagt i denne artikels stk. 1 og 2 og i artikel 36. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

5. Senest den 18. september 2015 og under hensyn til eksisterende praksis, standarder og EU-retsakter definerer Kommissionen ved hjælp af gennemførelsesretsakter referenceformater for avancerede elektroniske segl eller referencemetoder, når der anvendes alternative formater. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

Artikel 38

Kvalificerede certifikater for elektroniske segl

1. Kvalificerede certifikater for elektroniske segl skal opfylde kravene i bilag III.

2. Kvalificerede certifikater for elektroniske segl må ikke undergives ufravigelige krav, der går videre end kravene i bilag III.

3. Kvalificerede certifikater for elektroniske segl kan omfatte ikkeobligatoriske supplerende særlige kendetegn. Disse kendetegn må ikke påvirke interoperabiliteten mellem og anerkendelsen af kvalificerede elektroniske segl.

4. Såfremt et kvalificeret certifikat for elektronisk segl er blevet spærret efter den første aktivering, mister det sin gyldighed fra tidspunktet for spærringen, og dets status kan under ingen omstændigheder ændres.

5. Medlemsstaterne kan fastsætte nationale regler for en midlertidig suspension af kvalificerede certifikater for elektroniske segl på følgende betingelser:

a) hvis et kvalificeret certifikat for elektronisk segl er blevet suspenderet midlertidigt, mister det sin gyldighed i suspensionsperioden

b) suspensionsperioden angives klart i certifikatdatabasen og suspensionsstatus gøres synlig i suspensionsperioden af den tjeneste, der formidler oplysninger om status for certifikatet.

6. Kommissionen kan ved hjælp af gennemførelsesretsakter opstille referencenumre på standarder for kvalificerede certifikater for elektroniske segl. Et kvalificeret certifikat for elektroniske segl, der opfylder disse standarder, formodes at overholde kravene i bilag III. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

Artikel 39

Kvalificerede elektroniske seglgenereringssystemer

1. Artikel 29 finder tilsvarende anvendelse for så vidt angår kravene til kvalificerede elektroniske seglgenereringssystemer.

2. Artikel 30 finder tilsvarende anvendelse for så vidt angår certificering af kvalificerede elektroniske seglgenereringssystemer.

3. Artikel 31 finder tilsvarende anvendelse for så vidt angår offentliggørelse af en liste over certificerede kvalificerede elektroniske seglgenereringssystemer.

Artikel 40

Validering og bevaring af kvalificerede elektroniske segl

Artikel 32, 33 og 34 finder tilsvarende anvendelse for så vidt angår validering og bevaring af kvalificerede elektroniske segl.

AFDELING 6

Elektroniske tidsstempler

Artikel 41

Retsvirkninger af elektroniske tidsstempler

1. Et elektronisk tidsstempel må ikke nægtes retsvirkning og anerkendelse som bevis under retssager, alene af den grund at det er i elektronisk form, eller at det ikke opfylder kravene til et kvalificeret elektronisk tidsstempel.

2. For et kvalificeret elektronisk tidsstempel gælder der en formodning for nøjagtigheden af den dato og det tidspunkt, som det angiver, og integriteten af de data, som dato- og tidsangivelsen er knyttet til.

3. Et kvalificeret elektronisk tidsstempel, som er udstedt i en medlemsstat, anerkendes som et kvalificeret elektronisk tidsstempel i alle medlemsstater.

Artikel 42

Krav til kvalificerede elektroniske tidsstempler

1. Kvalificerede elektroniske tidsstempler skal opfylde følgende krav:

a) de forbinder dato og tidspunkt med data på en sådan måde, at det med rimelighed udelukker muligheden for at ændre dataene, uden at det opdages

b) de bygger på en præcis tidskilde forbundet med koordineret universaltid, og

c) de er forsynet med den kvalificerede tillidstjenesteudbyders avancerede elektroniske signatur eller forseglet med dennes avancerede elektroniske segl eller med en anden tilsvarende metode.

2. Kommissionen kan ved hjælp af gennemførelsesretsakter opstille referencenumre på standarder for forbindelsen af dato og tidspunkt med data og for brug af nøjagtige tidskilder. Forbindelsen af dato og tidspunkt med data og nøjagtige tidskilder, der opfylder disse standarder, formodes at overholde kravene i stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

AFDELING 7

Elektroniske registrerede leveringstjenester

Artikel 43

Retsvirkning af elektroniske registrerede leveringstjenester

1. Data, der sendes og modtages via en elektronisk registreret leveringstjeneste, må ikke nægtes retsvirkning og anerkendelse som bevismateriale under retssager, alene af den grund at de er i en elektronisk form, eller at de ikke opfylder kravene til den kvalificerede, elektroniske registrerede leveringstjeneste.

2. Med hensyn til data, der sendes og modtages via en kvalificeret elektronisk registreret leveringstjeneste, gælder der en formodning om dataenes integritet, den valgte afsenders afsendelse og den valgte modtagers modtagelse af dataene og nøjagtigheden af den dato og det tidspunkt for afsendelse og modtagelse, som den kvalificerede elektroniske registrerede leveringstjeneste angiver.

Artikel 44

Krav til kvalificerede elektroniske registrerede leveringstjenester

1. Kvalificerede elektroniske registrerede leveringstjenester skal opfylde følgende krav:

a) de udbydes af en eller flere kvalificerede tillidstjenesteudbydere

b) de sikrer med en høj grad af tillid identifikation af afsenderen

c) de sikrer forud for levering af dataene identifikation af modtageren

d) afsendelsen og modtagelsen af data er beskyttet af en kvalificeret tillidstjenesteudbyders avancerede elektroniske signatur eller avancerede elektroniske segl på en sådan måde, at det er umuligt at ændre dataene, uden at det opdages

e) hvis det er nødvendigt at ændre dataene, for at de kan sendes eller modtages, angives dette klart over for afsenderen og modtageren af dataene

f) datoen og tidspunktet for afsendelse, modtagelse og en eventuel ændring af data angives ved hjælp af et kvalificeret elektronisk tidsstempel.

Overføres dataene mellem to eller flere kvalificerede tillidstjenesteudbydere, gælder kravene i litra a)-f) for samtlige kvalificerede tillidstjenesteudbydere.

2. Kommissionen kan ved hjælp af gennemførelsesretsakter opstille referencenumre på standarder for dataafsendelses- og -modtagelsesprocesser. En dataafsendelses- og -modtagelsesproces, der opfylder disse standarder, formodes at overholde kravene i stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

AFDELING 8

Webstedsautentifikation

Artikel 45

Krav til kvalificerede certifikater for webstedsautentifikation

1. Kvalificerede certifikater for webstedsautentifikation skal opfylde kravene i bilag IV.

2. Kommissionen kan ved hjælp af gennemførelsesretsakter opstille referencenumre på standarder for kvalificerede certifikater for webstedsautentifikation. Et kvalificeret certifikat for webstedsautentifikation, der opfylder disse standarder, formodes at overholde kravene i bilag IV. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

KAPITEL IV

ELEKTRONISKE DOKUMENTER

Artikel 46

Retsvirkninger af elektroniske dokumenter

Et elektronisk dokument må ikke nægtes retsvirkning og anerkendelse som bevis under retssager, alene af den grund at det er i elektronisk form.

KAPITEL V

DELEGEREDE BEFØJELSER OG GENNEMFØRELSESBESTEMMELSER

Artikel 47

Udøvelse af de delegerede beføjelser

1. Beføjelsen til at vedtage delegerede retsakter tillægges Kommissionen på de i denne artikel fastlagte betingelser.

2. Beføjelsen til at vedtage delegerede retsakter, jf. artikel 30, stk. 4, tillægges Kommissionen for en ubegrænset periode fra den 17. september 2014.

3. Den i artikel 30, stk. 4, omhandlede delegation af beføjelser kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om spærring bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Afgørelsen får virkning fra dagen efter offentliggørelsen i *Den Europæiske Unions Tidende* eller fra en senere dato, der fastsættes nærmere i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.

4. Så snart Kommissionen vedtager en delegeret retsakt, giver den samtidigt Europa-Parlamentet og Rådet meddelelse herom.

5. En delegeret retsakt vedtaget i henhold til artikel 30, stk. 4, træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på to måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har informeret Kommissionen om, at de ikke agter at gøre indsigelse. Denne frist forlænges med to måneder på Europa-Parlamentets eller Rådets initiativ.

Artikel 48

Udvalgsprocedure

1. Kommissionen bistås af et udvalg. Dette udvalg er et udvalg som omhandlet i forordning (EU) nr. 182/2011.

2. Når der henvises til dette stykke, anvendes artikel 5 i forordning (EU) nr. 182/2011.

KAPITEL VI

AFSLUTTENDE BESTEMMELSER

Artikel 49

Revision

Kommissionen reviderer anvendelsen af denne forordning og aflægger rapport til Europa-Parlamentet og Rådet senest den 1. juli 2020. Kommissionen evaluerer navnlig, hvorvidt det er hensigtsmæssigt at ændre denne forordnings anvendelsesområde eller de specifikke bestemmelser heri, herunder artikel 6, artikel 7, litra f), samt artikel 34, 43, 44 og 45, under hensyntagen til de erfaringer, der er gjort med anvendelsen af denne forordning, og til den teknologiske, markedsmæssige og retlige udvikling.

Den i stk. 1 omhandlede rapport ledsages om nødvendigt af lovgivningsmæssige forslag.

Kommissionen forelægger endvidere hvert fjerde år efter udarbejdelsen af den i stk. 1 omhandlede rapport Europa-Parlamentet og Rådet en rapport om de fremskridt, der er gjort med hensyn til at opfylde målene for denne forordning.

Artikel 50

Ophævelse

1. Direktiv 1999/93/EF ophæves med virkning fra den 1. juli 2016.

2. Henvisninger til det ophævede direktiv betragtes som henvisninger til nærværende forordning.

Artikel 51

Overgangsforanstaltninger

1. Sikre signaturgenereringssystemer, for hvilke det er fastslået, at de opfylder kravene i artikel 3, stk. 4, i direktiv 1999/93/EF, anses for kvalificerede elektroniske signaturgenereringssystemer i henhold til nærværende forordning.

2. Kvalificerede certifikater, der er udstedt til fysiske personer i henhold til direktiv 1999/93/EF, anses for kvalificerede certifikater for elektroniske signaturer i henhold til nærværende forordning, indtil de udløber.

3. En certificeringstjenesteudbyder, der udsteder kvalificerede certifikater i henhold til direktiv 1999/93/EF, forelægger en overensstemmelsesvurderingsrapport for tilsynsorganet så hurtigt som muligt dog senest den 1. juli 2017. Indtil forelæggelsen af en sådan overensstemmelsesvurderingsrapport og tilsynsorganets gennemførelse af sin vurdering betragtes den pågældende certificeringstjenesteudbyder som en kvalificeret tillidstjenesteudbyder i henhold til nærværende forordning.

4. Forelægger en certificeringstjenesteudbyder, der udsteder kvalificerede certifikater i henhold til direktiv 1999/93/EF ikke en overensstemmelsesvurderingsrapport for tilsynsorganet inden for den i stk. 3 omhandlede frist, betragtes den pågældende certificeringstjenesteudbyder ikke som en kvalificeret tillidstjenesteudbyder i henhold til denne forordning fra den 2. juli 2017.

Artikel 52

Ikrafttræden

1. Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

2. Denne forordning anvendes fra den 1. juli 2016, bortset fra følgende bestemmelser:

a) artikel 8, stk. 3, artikel 9, stk. 5, artikel 12, stk. 2-9, artikel 17, stk. 8, artikel 19, stk. 4, artikel 20, stk. 4, artikel 21, stk. 4, artikel 22, stk. 5, artikel 23, stk. 3, artikel 24, stk. 5, artikel 27, stk. 4 og 5, artikel 28, stk. 6, artikel 29, stk. 2, artikel 30, stk. 3 og 4, artikel 31, stk. 3, artikel 32, stk. 3, artikel 33, stk. 2, artikel 34, stk. 2, artikel 37, stk. 4 og 5, artikel 38, stk. 6, artikel 42, stk. 2, artikel 44, stk. 2, artikel 45, stk. 2, artikel 47 and 48 finder anvendelse fra den 17. september 2014

b) artikel 7, artikel 8, stk. 1 og 2, artikel 9, 10, 11 og artikel 12, stk. 1, finder anvendelse fra datoen for anvendelsen af de i artikel 8, stk. 3, og artikel 12, stk. 8, omhandlede gennemførelsesretsakter

c) artikel 6 finder anvendelse fra tre år efter datoen for anvendelsen af de i artikel 8, stk. 3, og artikel 12, stk. 8, omhandlede gennemførelsesretsakter.

3. Opføres den anmeldte elektroniske identifikationsordning på den liste, som Kommissionen offentliggør i henhold til artikel 9, før den i stk. 2, litra c), i nærværende artikel omhandlede dato, sker anerkendelsen af det elektroniske identifikationsmiddel i medfør af denne ordning i henhold til artikel 6 senest 12 måneder efter offentliggørelsen af denne ordning, dog ikke før den i stk. 2, litra c), i nærværende artikel omhandlede dato.

4. Uanset stk. 2, litra c), i nærværende artikel kan en medlemsstat beslutte, at et elektronisk identifikationsmiddel i medfør af den elektroniske identifikationsordning, som en anden medlemsstat har anmeldt i henhold til artikel 9, stk. 1, anerkendes i den første medlemsstat fra datoen for anvendelsen af de i artikel 8, stk. 3, og artikel 12, stk. 8, omhandlede gennemførelsesretsakter. De pågældende medlemsstater underretter Kommissionen. Kommissionen offentliggør disse oplysninger.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 23. juli 2014.

På Europa-Parlamentets vegne	*På Rådets vegne*
M. SCHULZ	S. GOZI
Formand	*Formand*

BILAG I

KRAV TIL KVALIFICEREDE CERTIFIKATER FOR ELEKTRONISKE SIGNATURER

Kvalificerede certifikater for elektroniske signaturer skal indeholde:

a) en angivelse — som minimum i en form, der egner sig til automatiseret behandling — af, at certifikatet er udstedt som et kvalificeret certifikat for elektronisk signatur

b) et sæt data, der entydigt repræsenterer den kvalificerede tillidstjenesteudbyder, som udsteder de kvalificerede certifikater, herunder som minimum oplysning om, hvilken medlemsstat den pågældende udbyder er hjemmehørende i, og

— for en juridisk person: navn og, når det er relevant, registreringsnummer, som det fremgår af det officielle register

— for en fysisk person: personens navn

c) som minimum underskriverens navn eller pseudonym; anvendes der pseudonym, skal dette tydeligt angives

d) elektroniske signaturvalderingsdata, som svarer til dataene til de elektroniske signaturgenereringsdata

e) certifikatets ikrafttrædelses- og udløbsdato

f) certifikatets identifikationskode, der skal være entydig for den kvalificerede tillidstjenesteudbyder

g) den udstedende kvalificerede tillidstjenesteudbyders avancerede elektroniske signatur eller avancerede elektroniske segl

h) oplysninger om, hvor certifikatet for den avancerede elektroniske signatur eller det avancerede elektroniske segl, der henvises til i litra g), er gratis tilgængeligt

i) oplysninger om, hvor de tjenester, hvortil der kan rettes forespørgsel om det kvalificerede certifikats gyldighedsstatus, befinder sig

j) hvis de elektroniske signaturgenereringsdata, der svarer til de elektroniske signaturvalideringsdata, befinder sig i et kvalificeret elektronisk signaturgenereringssystem er: en passende angivelse af dette, som minimum i en form, der egner sig til automatiseret behandling.

BILAG II

KRAV TIL KVALIFICEREDE ELEKTRONISKE SIGNATURGENERERINGSSYSTEMER

1. Kvalificerede elektroniske signaturgenereringssystemer sikrer ved hjælp af passende tekniske og proceduremæssige midler som minimum, at:

   a) de elektroniske signaturgenereringsdata, der anvendes til elektronisk signaturgenerering, med rimelig sikkerhed forbliver fortrolige

   b) de elektroniske signaturgenereringsdata, der anvendes til elektronisk signaturgenerering, i praksis kun kan forekomme én gang

   c) de elektroniske signaturgenereringsdata, der anvendes til elektronisk signaturgenerering, med rimelig sikkerhed ikke kan udledes, og at den elektroniske signatur på pålidelig vis er beskyttet mod forfalskning under anvendelse af eksisterende teknologi

   d) de elektroniske signaturgenereringsdata, der anvendes til elektronisk signaturgenerering, på pålidelig vis kan beskyttes af den retmæssige underskriver mod andres brug.

2. Kvalificerede elektroniske signaturgenereringssystemer må ikke ændre de data, som skal underskrives, eller hindre, at disse data vises for underskriveren forud for signaturprocessen.

3. Generering og forvaltning af elektroniske signaturgenereringsdata på underskriverens vegne må kun udføres af en kvalificeret tillidstjenesteudbyder.

4. Uanset punkt 1, litra d), må kvalificerede tillidstjenesteudbydere, der forvalter elektroniske signaturgenereringsdata på underskriverens vegne, kun kopiere disse data til backupformål, forudsat at følgende betingelser er opfyldt:

   a) der skal opretholdes samme niveau af sikkerhed for kopierede datasæt som for de originale datasæt

   b) antallet af kopierede datasæt må ikke overstige det minimum, der er nødvendigt for at sikre tjenestens kontinuitet.

BILAG III

KRAV TIL KVALIFICEREDE CERTIFIKATER FOR ELEKTRONISKE SEGL

Kvalificerede certifikater for elektroniske segl skal indeholde:

a) en angivelse — som minimum i en form, der egner sig til automatiseret behandling — af, at certifikatet er udstedt som et kvalificeret certifikat for elektronisk segl

b) et sæt data, der entydigt repræsenterer den kvalificerede tillidstjenesteudbyder, som udsteder de kvalificerede certifikater, herunder som minimum oplysning om, hvilken medlemsstat den pågældende udbyder er hjemmehørende i, og

— for en juridisk person: navn og, når det er relevant, registreringsnummer, som det fremgår af det officielle register

— for en fysisk person: personens navn

c) som minimum navnet på den forseglende part og, når det er relevant, registreringsnummer, som det fremgår af det officielle register

d) elektroniske seglvalideringsdata, som svarer tilde elektroniske seglgenereringsdata

e) certifikatets ikrafttrædelses- og udløbsdato

f) certifikatets identifikationskode, der skal være entydig for den kvalificerede tillidstjenesteudbyder

g) den udstedende kvalificerede tillidstjenesteudbyders avancerede elektroniske signatur eller avancerede elektroniske segl

h) oplysninger om, hvor certifikatet for den avancerede elektroniske signatur eller det avancerede elektroniske segl, der henvises til i litra g), er gratis tilgængeligt

i) oplysninger om, hvor de tjenester, hvortil der kan rettes forespørgsel om det kvalificerede certifikats gyldighedsstatus, befinder sig

j) hvis de elektroniske seglgenereringsdata, der svarer til de elektroniske seglvalideringsdata, befinder sig i et kvalificeret elektronisk seglgenereringssystem: en passende angivelse af dette, som minimum i en form, der egner sig til automatiseret behandling.

BILAG IV

KRAV TIL KVALIFICEREDE CERTIFIKATER FOR WEBSTEDSAUTENTIFIKATION

Kvalificerede certifikater for webstedsautentifikation skal indeholde:

a) en angivelse — som minimum i en form, der egner sig til automatiseret behandling — af, at certifikatet er udstedt som et kvalificeret certifikat for webstedsautentifikation

b) et sæt data, der entydigt repræsenterer den kvalificerede tillidstjenesteudbyder, som udsteder de kvalificerede certifikater, herunder som minimum oplysning om, hvilken medlemsstat den pågældende udbyder er hjemmehørende i, og

— for en juridisk person: navn og, når det er relevant, registreringsnummer, som det fremgår af det officielle register

— for en fysisk person: personens navn

c) for fysiske personer: som minimum navnet på den person, som certifikatet er udstedt til, eller et pseudonym. Hvis der anvendes pseudonym, angives dette klart

for juridiske personer: som minimum navnet på den juridiske person, som certifikatet er udstedt til, og, når det er relevant, registreringsnummer, som det fremgår af det officielle register

d) adresseoplysninger, herunder som minimum oplysninger om by og nationalstat, for den fysiske eller juridiske person, som certifikatet er udstedt til, og, når det er relevant, som de fremgår af det officielle register

e) domænenavnet på det eller de domæner, der drives af den fysiske eller juridiske person, som certifikatet er udstedt til

f) certifikatets ikrafttrædelses- og udløbsdato

g) certifikatets identifikationskode, der skal være entydig for den kvalificerede tillidstjenesteudbyder

h) den udstedende kvalificerede tillidstjenesteudbyders avancerede elektroniske signatur eller avancerede elektroniske segl

i) oplysninger om, hvor certifikatet for den avancerede elektroniske signatur eller det avancerede elektroniske segl, der henvises til i litra h), er gratis tilgængeligt

j) oplysninger om, hvor de tjenester, hvortil der kan rettes forespørgsel om det kvalificerede certifikats gyldighedsstatus, befinder sig.