EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS (EL) nr 910/2014,

23. juuli 2014,

e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 114,

võttes arvesse Euroopa Komisjoni ettepanekut,

olles edastanud seadusandliku akti eelnõu liikmesriikide parlamentidele,

võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust ([1]),

toimides seadusandliku tavamenetluse kohaselt ([2])

ning arvestades järgmist:

(1) Usalduse loomine internetikeskkonnas on majandusliku ja sotsiaalse arengu alus. Usalduse puudumise tõttu, mida eelkõige põhjustab arvatav õiguskindluse puudumine, on tarbijad, ettevõtjad ja ametiasutused elektrooniliste tehingute tegemise ja uute teenuste kasutuselevõtu suhtes ebalevad.

(2) Käesoleva määruse eesmärk on suurendada usaldust elektrooniliste tehingute vastu siseturul, luues ühise aluse turvalisele elektroonilisele suhtlusele kodanike, ettevõtjate ja ametiasutuste vahel, suurendades sellega avaliku ja erasektori internetipõhiste teenuste, e-äri ja e-kaubanduse tõhusust liidus.

(3) Euroopa Parlamendi ja nõukogu direktiivis 1999/93/EÜ ([3]) käsitletakse e-allkirju, kuid seal ei ole esitatud kõikehõlmavat piiri- ja sektoriülest raamistikku turvaliste, usaldusväärsete ja kasutajasõbralike e-tehingute jaoks. Käesoleva määrusega täiendatakse ja laiendatakse nimetatud direktiivi *acquis*'d.

(4) Komisjoni 26. augusti 2010. aasta teatises „Euroopa digitaalarengu tegevuskava" on digitaalse majanduse positiivse mõjuringi tekkimise peamiste takistustena nimetatud digitaalse turu killustatust, koosvõime puudumist ja küberkuritegevuse kasvu. ELi kodakondsust käsitlevas 2010. aasta aruandes „ELi kodanike õigusi piiravate takistuste kõrvaldamine" rõhutas komisjon veelgi vajadust lahendada peamised probleemid, mis takistavad liidu kodanikel digitaalse ühtse turu ja piiriüleste digitaalteenuste eeliste kasutamist.

(5) Euroopa Ülemkogu soovitas oma 4. veebruari ja 23. oktoobri 2011. aasta järeldustes komisjonil luua 2015. aastaks digitaalne ühtne turg kiirete edusammude tegemiseks digitaalmajanduse võtmetähtsusega valdkondades ja täielikult integreeritud digitaalse ühtse turu edendamiseks, lihtsustades internetipõhiste teenuste piiriülest kasutamist ja pöörates erilist tähelepanu turvalise e-identimise ja e-autentimise hõlbustamisele.

([1]) ELT C 351, 15.11.2012, lk 73.
([2]) Euroopa Parlamendi 3. aprilli 2014. aasta seisukoht (*Euroopa Liidu Teatajas* seni avaldamata) ja nõukogu 23. juuli 2014. aasta otsus.
([3]) Euroopa Parlamendi ja nõukogu 13. detsembri 1999. aasta direktiiv 1999/93/EÜ elektroonilisi allkirju käsitleva ühenduse raamistiku kohta (EÜT L 13, 19.1.2000, lk 12).

(6) Oma 27. mai 2011. aasta järeldustes palus nõukogu komisjonil edendada digitaalset ühtset turgu sobivate tingimuste loomisega piiriüleste põhieelduste, näiteks e-identimise, e-dokumentide, e-allkirjade ja e-andmevahetusteenuste vastastikuseks tunnustamiseks ning koosvõimelisteks e-valitsuse teenusteks kogu Euroopa Liidus.

(7) Oma 21. septembri 2010. aasta resolutsioonis e-kaubanduse siseturu väljakujundamise kohta ([1]) rõhutas Euroopa Parlament elektrooniliste teenuste, eelkõige e-allkirja turvalisuse tähtsust ja vajadust luua avaliku võtme infrastruktuur (PKI) üleeuroopalisel tasandil ning palus komisjonil luua Euroopa valideerimisasutuste portaal eesmärgiga tagada e-allkirja piiriülene koosvõime ja suurendada internetis tehtavate tehingute turvalisust.

(8) Euroopa Parlamendi ja nõukogu direktiivis 2006/123/EÜ ([2]) nõutakse liikmesriikidelt ühtsete kontaktpunktide loomist selle tagamiseks, et kõiki teenuste osutamise valdkonnas tegutsemise alustamise ja selles valdkonnas tegutsemisega seotud toiminguid ja formaalsusi oleks lihtne teha eemalt elektrooniliste vahendite abil sobiva ühtse kontaktpunkti kaudu ja koos asjaomaste ametiasutustega. Paljud ühtsete kontaktpunktide kaudu kättesaadavad internetipõhised teenused eeldavad e-identimist, e-autentimist ja e-allkirja.

(9) Enamasti ei saa kodanikud kasutada e-identimist enda autentimiseks teises liikmesriigis, sest nende koduriigi riiklikke e-identimise süsteeme teistes liikmesriikides ei tunnustata. Selline elektrooniline takistus ei lase teenuseosutajatel siseturust täit kasu saada. Vastastikku tunnustatavad e-identimise vahendid lihtsustavad paljude teenuste piiriülest osutamist siseturul ja võimaldavad ettevõtjatel piiriüleselt tegutseda, ilma et neil oleks palju takistusi avaliku sektori asutustega suhtlemisel.

(10) Euroopa Parlamendi ja nõukogu direktiivis 2011/24/EL ([3]) luuakse e-tervise eest vastutavate riiklike asutuste võrgustik. Võrgustik peab piiriüleste tervishoiuteenuste turvalisuse ja järjepidevuse suurendamiseks koostama suunised piiriüleseks juurdepääsuks elektroonilistele tervishoiuandmetele ja -teenustele, muu hulgas toetades liikmesriike „ühiste identifitseerimis- ja autentimismeetmete väljatöötamisel, et hõlbustada piiriüleste tervishoiuteenuste osutamisel andmete edastamist". E-identimise ja e-autentimise vastastikune tunnustamine on põhitegur, et muuta piiriülesed tervishoiuteenused Euroopa kodanike jaoks tegelikkuseks. Kui inimesed sõidavad ravi saamiseks teise riiki, peavad nende meditsiinilised andmed olema ravi osutavas riigis kättesaadavad. See eeldab kindlat, turvalist ja usaldusväärset e-identimise raamistikku.

(11) Käesolevat määrust tuleks kohaldada täielikus vastavuses isikuandmete kaitse põhimõtetega, mis on sätestatud Euroopa Parlamendi ja nõukogu direktiivis 95/46/EÜ ([4]). Seda arvesse võttes tuleks käesoleva määrusega kehtestatud vastastikuse tunnustamise põhimõtte kohaselt internetipõhise teenuse jaoks tehtava autentimise käigus töödelda ainult selliseid tuvastamisandmeid, mis on piisavad, asjakohased ega ületa asjaomasele teenusele internetipõhise juurdepääsu võimaldamiseks vajalikku. Samuti peaksid direktiivis 95/46/EÜ sätestatud töötlemise konfidentsiaalsuse ja turvalisuse nõuetest kinni pidama usaldusteenuse osutajad ja järelevalveasutused.

(12) Üks käesoleva määruse eesmärke on kõrvaldada praegused takistused vähemalt e-identimise vahendite piiriüleselt kasutamiselt, mida liikmesriikides kasutatakse avalike teenuste autentimisel. Käesoleva määruse eesmärk ei ole sekkuda liikmesriikides loodud e-identiteedi haldamise süsteemide ja nendega seotud taristute küsimuses. Määruse eesmärk on tagada, et juurdepääsul liikmesriikide pakutavatele piiriülestele internetipõhistele teenustele oleks võimalik turvaline e-identimine ja e-autentimine.

([1]) ELT C 50 E, 21.2.2012, lk 1.
([2]) Euroopa Parlamendi ja nõukogu 12. detsembri 2006. aasta direktiiv 2006/123/EÜ teenuste kohta siseturul (ELT L 376, 27.12.2006, lk 36).
([3]) Euroopa Parlamendi ja nõukogu 9. märtsi 2011. aasta direktiiv 2011/24/EL patsiendiõiguste kohaldamise kohta piiriüleses tervishoius (ELT L 88, 4.4.2011, lk 45).
([4]) Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (EÜT L 281, 23.11.1995, lk 31).

(13) Liikmesriikidele peaks jääma vabadus kasutada või juurutada e-identimise vahendeid juurdepääsuks internetipõhistele teenustele. Samuti peaks neil olema võimalus otsustada, kas kaasata nende vahendite pakkumisse ka erasektor. Liikmesriikidel ei peaks olema kohustust teavitada e-identimise süsteemidest komisjoni. Liikmesriikidel on võimalus valida, kas teavitada komisjoni kõikidest riigisiseselt vähemalt avalikele internetipõhistele teenustele juurdepääsuks kasutatavatest e-identimise süsteemidest, teha seda mõne süsteemi puhul või üldse mitte.

(14) Käesolevas määruses tuleb sätestada mõned tingimused selle kohta, milliseid e-identimise vahendeid peab tunnustama ja kuidas e-identimise süsteemidest peaks teavitama. Need tingimused peaksid aitama liikmesriikidel luua vajalikku usaldust üksteise e-identimise süsteemide vastu ning vastastikku tunnustada e-identimise vahendeid, mis kuuluvad nende teavitatud süsteemidesse. Vastastikuse tunnustamise põhimõtet tuleks rakendada juhul, kui teavitava liikmesriigi e-identimise süsteem täidab teavitamise tingimusi ja teavitus on avaldatud *Euroopa Liidu Teatajas*. Vastastikuse tunnustamise põhimõtet tuleks siiski järgida ainult internetipõhiste teenuste autentimisel. Juurdepääs kõnealustele internetipõhistele teenustele ja nende lõplik osutamine taotlejale peaksid olema tihedalt seotud õigusega selliseid teenuseid siseriiklikes õigusaktides sätestatud tingimustel tarbida.

(15) Kohustus tunnustada e-identimise vahendeid peaks puudutama ainult selliseid vahendeid, mille identiteedi tagatistase on võrdväärne kõnealuse internetipõhise teenuse puhul nõutava tasemega või on sellest kõrgem. Samuti tuleks kõnealust kohustust kohaldada vaid siis, kui asjaomane avaliku sektori asutus kasutab kõnealusele internetipõhisele teenusele juurdepääsuks tagatist, mille tase on märkimisväärne või kõrge. Kooskõlas liidu õigusega peaks liikmesriikidele jääma õigus tunnustada madalama identiteedi tagatistasemega e-identimise vahendeid.

(16) Tagatistasemed peaksid kajastama, mil määral on e-identimise vahend isikusamasuse tuvastamiseks usaldusväärne, andes seega kindluse, et ennast teatud isikuna esitlev isik on tõepoolest isik, kellele need isikuandmed on omistatud. Tagatistaseme liik sõltub sellest, mil määral on see e-identimise vahend usaldusväärne isiku väidetava või tema poolt kinnitatud isikusamasuse tuvastamiseks, võttes arvesse menetlusi (näiteks isikusamasuse tõendamine ja kontrollimine ning autentimine), haldustegevust (näiteks e-identimise vahendeid väljastav üksus ja selliste vahendite väljastamise menetlus) ja rakendatavat tehnilist kontrolli. Liidu rahastatud suurprojektide, standardimise ja rahvusvahelise tegevuse tulemusena on koostatud erinevaid tagatistasemete tehnilisi määratlusi ja kirjeldusi. Suurprojekt STORK ja ISO 29115 osutavad eelkõige muu hulgas tasemetele 2, 3 ja 4, mida tuleks igati arvesse võtta tehniliste miinimumnõuete, standardite ja menetluste kehtestamisel madala, märkimisväärse ja kõrge tagatistaseme jaoks käesoleva määruse tähenduses, tagades samal ajal käesoleva määruse järjekindla kohaldamise eelkõige kõrge tagatistaseme puhul, mis on seotud isikusamasuse tõendamisega kvalifitseeritud sertifikaatide väljastamisel. Kehtestatavad tingimused peaksid olema tehnoloogiliselt neutraalsed. Vajalikke turvanõudeid peaks olema võimalik saavutada erinevate tehnoloogiate abil.

(17) Liikmesriigid peaksid ergutama erasektorit vabatahtlikult kasutama teavitatud süsteemi kuuluvaid e-identimise vahendeid identimiseks, kui see on vajalik internetipõhiste teenuste või e-tehingute puhul. Võimalus kasutada kõnealuseid e-identimise vahendeid võimaldaks luua erasektoris usalduse paljudes liikmesriikides juba vähemalt avalike teenuste puhul laialdaselt kasutatava e-identimise ja e-autentimise vastu ning muuta piiriülese juurdepääsu erasektori internetipõhistele teenustele ettevõtjate ja kodanike jaoks lihtsamaks. Selleks et e-identimise vahendite piiriülest kasutamist erasektori jaoks lihtsamaks muuta, peaks liikmesriigi pakutav autentimisvõimalus olema väljaspool kõnealuse liikmesriigi territooriumi asuvatele erasektori tuginevatele isikutele kättesaadav samadel tingimustel kui kõnealuses liikmesriigis asuvatele erasektori tuginevatele isikutele. Seega võib teavitav liikmesriik erasektori tuginevate isikute puhul kindlaks määrata autentimisvahenditele juurdepääsu tingimused. Juurdepääsu tingimustes võib olla teade selle kohta, kas teavitatud süsteemi kuuluvad autentimisvahendid on erasektori tuginevatele isikutele juba kättesaadavad.

(18) Käesolevas määruses sätestatakse teavitava liikmesriigi, e-identimise vahendit väljastava osalise ja autentimismenetlust läbiviiva osalise vastutus käesolevast määrusest tulenevate asjakohaste kohustuste täitmata jätmise korral. Käesolevat määrust tuleks aga kohaldada kooskõlas siseriiklike vastutust käsitlevate eeskirjadega. Seega ei mõjuta see näiteks neid siseriiklikke eeskirju, mis puudutavad kahjude määratlust või asjakohaseid kohaldatavaid menetluseeskirju, sealhulgas tõendamiskohustust.

(19) E-identimise süsteemide turvalisus on põhitegur e-identimise süsteemide usaldusväärseks piiriüleseks vastastikuseks tunnustamiseks. Seoses sellega peaksid liikmesriigid tegema liidu tasandil koostööd e-identimise süsteemide koosvõime ja turvalisuse küsimustes. Juhul kui e-identimise süsteemid võivad nõuda tuginevatelt isikutelt teatava riist- või tarkvara kasutamist riigi tasandil, eeldab piiriülene koosvõime, et nimetatud liikmesriigid ei kehtestaks selliseid nõudeid väljaspool tema territooriumi asuvatele tuginevatele isikutele ega nõuaks nendega seonduvate kulude katmist. Sellisel juhul tuleks sobivaid lahendusi arutada ja need välja töötada koosvõime raamistiku piires. Teisalt ei ole võimalik vältida tehnilisi nõudeid, mis tulenevad riigisiseste e-identimise vahendite tehnilisest kirjeldusest ja mis tõenäoliselt mõjutavad selliste elektrooniliste vahendite (nt kiipkaardid) kasutajaid.

(20) Liikmesriikide koostöö peaks olema suunatud teavitatud e-identimise süsteemide tehnilisele koosvõimele, et soodustada usalduse ja turvalisuse kõrget taset, mis vastab riski astmele. Liikmesriikidevaheline teabevahetus ja parimate tavade jagamine nende vastastikuse tunnustamise eesmärgil peaks nimetatud koostööle kaasa aitama.

(21) Käesoleva määrusega tuleks luua ka üldine õigusraamistik usaldusteenuste kasutamiseks. Määrusega ei tuleks siiski kehtestada üldist kohustust neid teenuseid kasutada või rajada juurdepääsupunkt kõigi olemasolevate usaldusteenuste jaoks. Eelkõige ei peaks määrus hõlmama selliste teenuste osutamist, mida kindlaksmääratud hulk osalejaid kasutab eranditult suletud süsteemides ning mis ei mõjuta kolmandaid isikuid. Näiteks ei tuleks käesoleva määruse nõudeid kohaldada ettevõtete või avaliku halduse asutustes usaldusteenuseid kasutavate sisemenetluste haldamiseks loodud süsteemide suhtes. Käesolevas määruses sätestatud nõuetele peaksid vastama üksnes need üldsusele osutatavad usaldusteenused, mis mõjutavad kolmandaid isikuid. Samuti ei peaks käesolev määrus hõlmama lepingute sõlmimise ja kehtivuse või muude juriidiliste kohustuste tekkimise ja kehtivusega seotud aspekte, juhul kui vorminõuded on sätestatud siseriiklikus või liidu õiguses. Samuti ei peaks käesolev määrus mõjutama siseriiklikke vorminõudeid avalike registrite, eelkõige äriregistri ja kinnistusraamatu kohta.

(22) Selleks et soodustada usaldusteenuste üldist piiriülest kasutamist, peaks neid kõikides liikmesriikides olema võimalik kasutada tõendina kohtumenetlustes. Usaldusteenuste õiguslik toime tuleks kindlaks määrata siseriiklikus õiguses, juhul kui käesolevas määruses ei ole sätestatud teisiti.

(23) Kui käesoleva määrusega kehtestatakse kohustus tunnustada usaldusteenust, võib sellist usaldusteenust mitte tunnustada vaid juhul, kui adressaat ei ole võimeline seda kasutama või kontrollima tehnilistel põhjustel, mida adressaat mõjutada ei saa. Kõnealune kohustus ei peaks iseenesest siiski tingima nõuet, et avaliku sektori asutus soetaks kõigi olemasolevate usaldusteenuste tehnilist kasutamist võimaldava riist- või tarkvara.

(24) Liikmesriigid võivad säilitada või kehtestada usaldusteenuseid käsitlevaid liidu õigusega kooskõlas olevaid siseriiklikke õigusnorme, kui asjaomased teenused on käesoleva määrusega jäetud täielikult ühtlustamata. Käesoleva määrusega kooskõlas olevad usaldusteenused peaksid siiski olema siseturul vabas ringluses.

(25) Liikmesriikidel peaks olema vabadus lisaks käesolevas määruses sätestatud usaldusteenuste suletud nimekirja kuuluvatele usaldusteenustele kindlaks määrata muud liiki usaldusteenuseid, et neid tunnustataks riiklikul tasandil kvalifitseeritud usaldusteenustena.

(26) Arvestades tehnoloogiliste muutuste kiirust, tuleks käesolevas määruses kasutada uuendustele avatud lähenemisviisi.

(27) Käesolev määrus peaks olema tehnoloogiaküsimustes neutraalne. Selle õiguslik mõju peaks olema saavutatav mis tahes tehniliste vahenditega eeldusel, et täidetakse käesoleva määruse tingimusi.

(28) Selleks et suurendada eelkõige väikese ja keskmise suurusega ettevõtjate (VKEd) ja tarbijate usaldust siseturu vastu ning edendada usaldusteenuste ja -toodete kasutamist, tuleks nõuete ja kohustuste määratlemisel võtta kasutusele kvalifitseeritud usaldusteenuste ja kvalifitseeritud usaldusteenuse osutaja mõisted, mis tagavad kõigi kasutatavate või osutatavate kvalifitseeritud usaldusteenuste ja -toodete turvalisuse kõrge taseme.

(29) Vastavalt nõukogu otsusega 2010/48/EÜ ([1]) heaks kiidetud ÜRO puuetega inimeste õiguste konventsioonist, eelkõige konventsiooni artiklist 9 tulenevatele kohustustele peaksid puuetega inimesed saama kasutada usaldusteenuseid ja nende teenuste osutamisel kasutatavaid lõpptarbijale suunatud tooteid teiste tarbijatega võrdsetel alustel. Osutatavad usaldusteenused ja kõnealuste teenuste osutamisel kasutatavad lõpptarbijale suunatud tooted tuleks seega võimaluse korral teha puuetega inimestele juurdepääsetavaks. Teostatavusuuring peaks hõlmama muu hulgas tehnilisi ja majanduslikke kaalutlusi.

(30) Liikmesriigid peaksid määrama järelevalveasutuse või järelevalveasutused käesoleva määruse kohase järelevalve teostamiseks. Samuti peaks liikmesriikidel olema võimalik vastastikusel kokkuleppel teise liikmesriigiga otsustada määrata selle teostamiseks kõnealuses teises liikmesriigis asuv järelevalveasutus.

(31) Järelevalveasutused peaksid tegema andmekaitseasutustega koostööd, näiteks teavitades neid kvalifitseeritud usaldusteenuse osutajate auditite tulemustest, kui ilmneb, et isikuandmete kaitse eeskirju on rikutud. Teavitamine peaks hõlmama eelkõige turvaintsidente ja isikuandmetega seotud rikkumisi.

(32) Kõik usaldusteenuse osutajad on kohustatud kohaldama oma tegevusega seotud ohte arvestavaid häid turvatavasid, et suurendada kasutajate usaldust ühtse turu vastu.

(33) Sätted, mis käsitlevad varjunimede kasutamist sertifikaatidel, ei tohiks takistada liikmesriike nõudmast isikute tuvastamist liidu või siseriikliku õiguse kohaselt.

(34) Kõik liikmesriigid peaksid täitma olulisi ühiseid järelevalvenõudeid, et tagada kvalifitseeritud usaldusteenuste võrreldav turvatase. Selleks et hõlbustada nimetatud nõuete järjekindlat kohaldamist kogu liidus, peaksid liikmesriigid võtma kasutusele võrreldavad meetmed ning vahetama teavet oma järelevalvetoimingute ja parimate tavade kohta kõnealuses valdkonnas.

(35) Käesoleva määruse nõudeid, eelkõige turvalisust ja vastutust käsitlevaid sätteid, tuleks kohaldada kõigi usaldusteenuse osutajate suhtes, et tagada nende tegevuse ja teenustega seotud hoolsuskohustuse täitmine, läbipaistvus ja vastutus. Võttes arvesse usaldusteenuse osutajate poolt osutatavate teenuste liiki, on selliste nõuete puhul siiski kohane teha vahet kvalifitseeritud ja kvalifitseerimata usaldusteenuse osutajatel.

(36) Kõiki usaldusteenuse osutajaid hõlmava järelevalvekorra kehtestamine peaks tagama nende tegevuse ja teenuste turvalisusele ja nendega seotud vastutusele võrdsed tingimused, mis parandab kasutajate kaitset ja siseturu toimimist. Kvalifitseerimata usaldusteenuse osutajate suhtes tuleks kohaldada paindlikku ja reageerivat järgnevat järelevalvet, mis on nende teenuste ja tegevuse laadist tulenevalt põhjendatud. Seega ei peaks järelevalveasutusel olema üldist kohustust teostada järelevalvet kvalifitseerimata usaldusteenuse osutajate üle. Järelevalveasutus peaks võtma meetmeid vaid juhul, kui talle saab teatavaks (näiteks ta saab asjakohase teate kvalifitseerimata usaldusteenuse osutajalt endalt, teiselt järelevalveasutuselt, tema kasutajalt või äripartnerilt või see selgub järelevalveasutuse enda läbiviidud uurimise põhjal), et kvalifitseerimata usaldusteenuse osutaja ei vasta käesoleva määruse nõuetele.

([1]) Nõukogu 26. novembri 2009. aasta otsus 2010/48/EÜ Ühinenud Rahvaste Organisatsiooni puuetega inimeste õiguste konventsiooni sõlmimise kohta Euroopa Ühenduse nimel (ELT L 23, 27.1.2010, lk 35).

(37) Käesolevas määruses tuleks sätestada kõigi usaldusteenuse osutajate vastutus. Eelkõige kehtestatakse määrusega vastutuskord, mille kohaselt kõik usaldusteenuse osutajad peaksid vastutama füüsilisele või juriidilisele isikule põhjustatud kahju eest, mis tuleneb käesolevas määruses sätestatud kohustuste täitmata jätmisest. Selleks et hõlbustada sellise finantsriski hindamist, mida usaldusteenuse osutajatel tuleb võib-olla kanda või mille nad peaksid katma kindlustuspoliisidega, võivad usaldusteenuse osutajad käesoleva määruse kohaselt teatud tingimustel kehtestada nende osutatavate teenuste kasutamisele piirangud ja mitte vastutada kahju eest, mis tuleneb selliseid piiranguid ületavast teenuste kasutamisest. Kliente tuleks piirangutest eelnevalt nõuetekohaselt teavitada. Sellised piirangud peaksid olema kolmandale isikule arusaadavad, näiteks võib sellekohase piiranguid käsitleva teabe lisada osutatavate teenuste kasutamistingimustesse või kasutada muid arusaadavaid vahendeid. Nende põhimõtete jõustamisel tuleks käesolevat määrust kohaldada kooskõlas siseriiklike vastutust käsitlevate eeskirjadega. Seega ei mõjuta käesolev määrus näiteks siseriiklikke eeskirju, mis puudutavad kahjude määratlust, tahtlikkust, ettevaatamatust või asjakohaseid kohaldatavaid menetluseeskirju.

(38) Turvarikkumistest teatamine ja turvaohtude hindamine on väga oluline asjaomastele isikutele adekvaatse teabe andmisel turvarikkumise või tervikluse kao korral.

(39) Selleks et võimaldada komisjonil ja liikmesriikidel hinnata käesoleva määruse kehtestatud rikkumistest teatamise mehhanismi tõhusust, tuleks järelevalveasutustelt nõuda kokkuvõtliku teabe esitamist komisjonile ning Euroopa Liidu Võrgu- ja Infoturbeametile (ENISA).

(40) Selleks et võimaldada komisjonil ja liikmesriikidel hinnata käesoleva määrusega kehtestatud täiustatud järelevalvemehhanismi tõhusust, tuleks järelevalveasutustelt nõuda aruandeid nende tegevuse kohta. See aitaks oluliselt lihtsustada heade tavade vahetamist järelevalveasutuste vahel ja tagaks, et kõikides liikmesriikides kontrollitakse oluliste järelevalvenõuete järjekindlat ja tõhusat rakendamist.

(41) Selleks et tagada kvalifitseeritud usaldusteenuste jätkusuutlikkus ja püsivus ning suurendada kasutajate usaldust kvalifitseeritud usaldusteenuste järjepidevuse vastu, peaksid järelevalveasutused kontrollima lõpetamiskava käsitlevate sätete olemasolu ja nõuetekohast kohaldamist juhtudel, kui kvalifitseeritud usaldusteenuse osutajad lõpetavad oma tegevuse.

(42) Kvalifitseeritud usaldusteenuse osutajate üle järelevalve teostamise lihtsustamiseks näiteks juhul, kui teenuseosutaja pakub oma teenuseid teise liikmesriigi territooriumil ega ole seal järelevalve all, või juhul, kui teenuseosutaja arvutid asuvad mõne muu liikmesriigi territooriumil kui teenuseosutaja asukohaliikmesriik, tuleks luua liikmesriikide järelevalveasutuste vahelise vastastikuse abistamise süsteem.

(43) Selleks et tagada kvalifitseeritud usaldusteenuse osutajate ja nende osutatavate teenuste vastavus käesoleva määruse nõuetele, peaks vastavushindamisasutus teostama nende vastavushindamise ja kvalifitseeritud usaldusteenuse osutajad peaksid hindamise tulemusel valminud vastavushindamisaruande esitama järelevalveasutusele. Kui järelevalveasutus nõuab kvalifitseeritud usaldusteenuse osutajalt *ad hoc*-vastavushindamisaruande esitamist, peaks järelevalveasutus kinni pidama eelkõige hea valitsemistava põhimõttest, sealhulgas kohustusest oma otsuseid põhjendada, ning proportsionaalsuse põhimõttest. Seetõttu peaks järelevalveasutus nõuetekohaselt põhjendama oma otsust, millega nõutakse *ad hoc*-vastavushindamisaruande esitamist.

(44) Käesoleva määruse eesmärk on tagada ühtne raamistik usaldusteenuste turvalisuse ja õiguskindluse kõrge taseme kindlustamiseks. Seoses sellega peaks komisjon toodete ja teenuste vastavushindamise käsitlemisel püüdma vajaduse korral saavutada koostoimet asjakohaste olemasolevate Euroopa tasandi ja rahvusvaheliste kavadega, näiteks Euroopa Parlamendi ja nõukogu määrusega (EÜ) nr 765/2008, ([1]) milles sätestatakse vastavushindamisasutuste akrediteerimise ja toodete turujärelevalve nõuded.

([1]) Euroopa Parlamendi ja nõukogu 9. juuli 2008. aasta määrus (EÜ) nr 765/2008, millega sätestatakse akrediteerimise ja turujärelevalve nõuded seoses toodete turustamisega ja tunnistatakse kehtetuks määrus (EMÜ) nr 339/93 (ELT L 218, 13.8.2008, lk 30).

(45) Selleks et võimaldada tõhusat algatusprotsessi, mis viiks kvalifitseeritud usaldusteenuse osutajate ja nende pakutavate kvalifitseeritud usaldusteenuste usaldusnimekirja kandmiseni, tuleks ergutada eelsuhtlust tulevaste kvalifitseeritud usaldusteenuse osutajate ja pädevate järelevalveasutuste vahel, et lihtsustada hoolsuskohustuse täitmist, mis viib kvalifitseeritud usaldusteenuste osutamiseni.

(46) Usaldusnimekirjad on turu korraldajate vahelise usalduse loomisel väga olulised, sest need näitavad teenuseosutaja kvalifitseeritud staatust järelevalve ajal.

(47) Usaldus internetipõhiste teenuste vastu ja nende kasutamise mugavus on üliolulised selleks, et kasutajad saaksid e-teenustest täielikku kasu ja neid teadlikult kasutada. Selleks tuleks luua ELi usaldusmärk, mis tähistaks kvalifitseeritud usaldusteenuse osutajate poolt osutatavaid kvalifitseeritud usaldusteenuseid. Selline kvalifitseeritud usaldusteenuse osutajate ELi usaldusmärk eristaks kvalifitseeritud usaldusteenuseid selgelt teistest usaldusteenustest, aidates seega kaasa turu läbipaistvusele. ELi usaldusmärgi kasutamine kvalifitseeritud usaldusteenuse osutajate poolt peaks olema vabatahtlik ja sellest ei peaks tulenema muid nõudeid peale käesolevas määruses sätestatud nõuete.

(48) Kuigi e-allkirjade vastastikuse tunnustamise tagamiseks on vaja kõrget turvataset, tuleks teatavatel juhtudel, näiteks seoses komisjoni otsusega 2009/767/EÜ ([1]) tunnustada ka madalama turvatasemega e-allkirju.

(49) Käesoleva määrusega tuleks kehtestada põhimõte, et e-allkirja ei tohiks tunnistada õiguslikult kehtetuks seetõttu, et see on elektroonilisel kujul või ei vasta kvalifitseeritud e-allkirjadele esitatavatele nõuetele. E-allkirjade õiguslik toime peaks olema kindlaks määratud siseriiklikus õiguses, välja arvatud käesolevas määruses sätestatud nõue, mille kohaselt kvalifitseeritud e-allkirjal peaks olema käsitsi kirjutatud allkirjaga samaväärne õiguslik toime.

(50) Kuna praegu kasutavad liikmesriikide pädevad ametiasutused oma dokumentide elektrooniliseks allkirjastamiseks täiustatud e-allkirja erinevaid formaate, on vaja tagada, et liikmesriikidel on võimalik elektrooniliselt allkirjastatud dokumentide saamise korral tehniliselt toetada vähemalt teatavat hulka täiustatud e-allkirja formaate. Samamoodi tuleks tagada, et kui liikmesriikide pädevad asutused kasutavad täiustatud e-templit, toetaksid nad vähemalt teatavat hulka täiustatud e-templi formaate.

(51) Allkirja andja peaks saama usaldada kvalifitseeritud e-allkirja andmise vahendeid kolmanda isiku hooleks eeldusel, et rakendatakse asjakohaseid mehhanisme ja menetlusi selle tagamiseks, et üksnes allkirja andjal on kontroll oma e-allkirja andmiseks vajalike andmete üle, ning eeldusel, et vahendi kasutamisel täidetakse kvalifitseeritud e-allkirjadele esitatavaid nõudeid.

(52) E-allkirjade andmine vahemaa tagant, mille puhul e-allkirja andmise keskkonda haldab allkirja andja nimel usaldusteenuse osutaja, tõenäoliselt suureneb e-allkirja paljude majanduslike eeliste tõttu. Tagamaks, et sellised e-allkirjad tunnistatakse õiguslikult samaväärseks täielikult kasutaja hallatavas keskkonnas antud e-allkirjadega, peaksid vahemaa tagant e-allkirja andmise teenuse osutajad kohaldama konkreetseid turvalisi juhtimis- ja haldusmenetlusi ning kasutama usaldusväärseid süsteeme ja tooteid, sealhulgas turvalisi elektroonilise side kanaleid, et tagada e-allkirja andmise keskkonna usaldusväärsus ja sellise keskkonna kasutamine üksnes allkirja andja järelevalve all. Juhul kui kvalifitseeritud e-allkiri on antud vahemaa tagant e-allkirja andmise vahendiga, tuleks kohaldada käesoleva määrusega sätestatud kvalifitseeritud usaldusteenuse osutajate suhtes kohaldatavaid nõudeid.

([1]) Komisjoni 16. oktoobri 2009. aasta otsus 2009/767/EÜ, millega kehtestatakse meetmed elektrooniliste haldustoimingute kasutamise lihtsustamiseks nn ühtsete kontaktpunktide kaudu, mis on sätestatud Euroopa Parlamendi ja nõukogu direktiivis 2006/123/EÜ teenuste kohta siseturul (ELT L 274, 20.10.2009, lk 36).

(53) Kvalifitseeritud sertifikaatide peatamine on mitme liikmesriigi puhul usaldusteenuse osutajate seas kindlalt väljakujunenud tegevuspraktika, mis erineb tühistamisest ja mis toob kaasa sertifikaadi ajutise kehtetuse. Õiguskindluse huvides on vaja, et sertifikaadi peatatud staatus oleks alati selgesti märgitud. Seetõttu peaks usaldusteenuse osutajad olema kohustatud selgelt märkima sertifikaadi staatuse ja selle peatamise korral täpse ajavahemiku, mille jooksul sertifikaat on peatatud. Käesoleva määrusega ei tohiks usaldusteenuse osutajaid või liikmesriike kohustada sertifikaadi peatamist kasutama, vaid tuleks ette näha läbipaistvuseeskirjad juhtudeks, kui selline võimalus on olemas.

(54) Kvalifitseeritud sertifikaatide piiriülene koosvõime ja tunnustamine on kvalifitseeritud e-allkirjade piiriülese tunnustamise eelduseks. Seetõttu ei tohiks kvalifitseeritud sertifikaatide suhtes kohaldada ühtegi kohustuslikku nõuet, mis ületab käesolevas määruses sätestatud nõudeid. Riigi tasandil tuleks siiski lubada lisada kvalifitseeritud sertifikaatidele eritunnuseid, näiteks kordumatuid identifitseerimistunnuseid, eeldusel et sellised eritunnused ei takista kvalifitseeritud sertifikaatide ja e-allkirjade piiriülest koosvõimet ja tunnustamist.

(55) Rahvusvahelistel standarditel põhinev infotehnoloogia turvasertifitseerimine (näiteks ISO 15408 ja seonduvad hindamismeetodid ja vastastikuse tunnustamise kord) on oluline kvalifitseeritud e-allkirja andmise vahendi turvalisuse verifitseerimise vahend ja selle kasutamist tuleks edendada. Innovaatilised lahendused ja teenused, näiteks allkirja andmine mobiiltelefoniga ja pilvepõhiselt, tuginevad aga kvalifitseeritud allkirja andmise vahenditega seotud tehnilistele ja organisatoorsetele lahendustele, millele ei pruugi veel turvastandardit olla või mille esmane infotehnoloogia turvasertifitseerimine on pooleli. Kvalifitseeritud e-allkirja andmise vahendite turvalisuse taset võiks hinnata alternatiivsete protsesside abil üksnes juhul, kui turvastandardit ei ole või kui esmane infotehnoloogia turvasertifitseerimine on pooleli. Need protsessid peaksid olema võrreldavad infotehnoloogia turvasertifitseerimise standarditega, kui tegu on samaväärsete turvatasemetega. Selliste protsesside juures võiks olla kasu vastastikusest hindamisest.

(56) Käesolevas määruses tuleks sätestada nõuded kvalifitseeritud e-allkirja andmise vahenditele, et tagada täiustatud e-allkirjade toimivus. Käesoleva määrusega ei tuleks hõlmata kogu süsteemikeskkonda, milles sellised vahendid toimivad. Seetõttu tuleks kvalifitseeritud allkirja andmise vahendite sertifitseerimise kohaldamisel piirduda riistvara ja süsteemitarkvaraga, mida kasutatakse allkirja andmiseks kasutatavate andmete loomiseks, säilitamiseks või töötlemiseks allkirja andmise vahendis. Vastavalt asjaomastes standardites esitatule ei tohiks sertifitseerimise kohustus hõlmata allkirja andmise rakendusi.

(57) Allkirja kehtivusega seotud õiguskindluse tagamiseks on väga oluline täpsustada, milliseid kvalifitseeritud e-allkirja osi peaks valideeriv tuginev isik hindama. Lisaks peaks selliste nõuete määratlemine, mida esitatakse kvalifitseeritud usaldusteenuse osutajatele, kes võivad osutada kvalifitseeritud valideerimisteenust tuginevatele isikutele, kes ei soovi või ei saa ise kvalifitseeritud e-allkirju valideerida, innustama era- ja avalikku sektorit sellistesse teenustesse investeerima. Need mõlemad asjaolud peaksid muutma kvalifitseeritud e-allkirjade valideerimise liidu tasandil lihtsaks ja mugavaks kõigile osalistele.

(58) Kui tehingu tegemine eeldab juriidilise isiku kvalifitseeritud e-templit, peaks samavõrra aktsepteeritav olema ka juriidilise isiku volitatud esindaja kvalifitseeritud e-allkiri.

(59) E-tempel peaks olema tõend selle kohta, et e-dokumendi on väljastanud juriidiline isik, ning tagama kindluse dokumendi päritolu ja tervikluse suhtes.

(60) E-templi kvalifitseeritud sertifikaate väljastavad usaldusteenuse osutajad peaksid rakendama vajalikud meetmed, mis võimaldavad teha kindlaks juriidilist isikut esindava füüsilise isiku, kellele e-templi kvalifitseeritud sertifikaat väljastatakse, juhul kui selline kindlakstegemine on riigi tasandil vajalik seoses haldus- või kohtumenetlustega.

(61) Käesoleva määrusega tuleks tagada teabe pikaajaline säilitamine, et tagada e-allkirjade ja e-templite õiguslik kehtivus pika aja jooksul, ning garanteerida võimalus neid valideerida sõltumata tehnoloogia arengust tulevikus.

(62) Kvalifitseeritud e-ajatemplite turvalisuse tagamiseks tuleks käesolevas määruses nõuda täiustatud e-templi või täiustatud e-allkirja või teiste samaväärsete meetodite kasutamist. On tõenäoline, et innovatsioon viib uute tehnoloogiateni, mis võivad tagada ajatemplite turvalisuse samaväärsel tasemel. Kui kasutatakse teisi meetodeid peale täiustatud e-templi või täiustatud e-allkirja, peaks kvalifitseeritud usaldusteenuse osutaja vastavushindamisaruandes tõendama, et selline meetod tagab samaväärse turvalisuse taseme ja vastab käesolevas määruses sätestatud kohustustele.

(63) E-dokumendid on olulised piiriüleste e-tehingute edasiarendamiseks siseturul. Selle tagamiseks, et e-tehingut ei lükata tagasi ainuüksi seetõttu, et dokument on elektroonilisel kujul, tuleks käesoleva määrusega kehtestada põhimõte, et e-dokumenti ei tohiks tunnistada õiguslikult kehtetuks põhjusel, et see on elektroonilisel kujul.

(64) Täiustatud e-allkirja ja e-templi formaatide käsitlemisel peaks komisjon tuginema olemasolevatele tavadele, standarditele ja õigusnormidele, eelkõige komisjoni otsusele 2011/130/EL ([1]).

(65) E-templit võib lisaks juriidilise isiku väljastatud dokumendi autentimisele kasutada ka kõikide juriidilise isiku digitaalvarade, näiteks tarkvara või serverite autentimiseks.

(66) Oluline on luua õigusraamistik registreeritud e-andmevahetusteenusega seotud olemasolevate riiklike õigussüsteemide piiriülese tunnustamise hõlbustamiseks. Selline raamistik võiks avada liidu usaldusteenuste osutajatele uued turuvõimalused ka uute üleeuroopaliste registreeritud e-andmevahetusteenuste pakkumisel.

(67) Veebisaidi autentimisteenused pakuvad veebisaidi külastajale vahendi, mille abil teha kindlaks, et veebisait on ehtne ja seaduslik. Sellised teenused aitavad luua usaldust ja kindlustunnet internetipõhise äritegevuse suhtes, kuna autenditud veebisait on kasutajate jaoks usaldusväärne. Veebisaidi autentimisteenuste osutamine ja kasutamine on täiesti vabatahtlik. Selleks aga, et veebisaidi autentimisteenusest saaks usalduse suurendamise, kasutajakogemuse parandamise ja siseturu kasvu edendamise vahend, tuleks käesolevas määruses kehtestada teenuseosutajatele ja nende teenustele minimaalsed turvalisuse ja vastutusega seotud kohustused. Seetõttu on arvesse võetud olemasolevate tööstusharupoolsete algatuste, näiteks sertifitseerimisasutuste ja brauserite foorumi tulemusi. Lisaks ei tohiks käesolev määrus takistada teiste, käesoleva määruse kohaldamisalasse mittekuuluvate veebisaidi autentimisvahendite või meetodite kasutamist ega takistada kolmandate riikide veebisaidi autentimisteenuste pakkujaid liidus oma teenuseid pakkumast. Käesoleva määruse kohaselt tuleks kolmanda riigi teenuseosutaja veebisaidil pakutavaid autentimisteenuseid tunnustada kvalifitseeritud teenustena vaid juhul, kui liidu ja kolmanda riigi vahel, kus teenuseosutaja on asutatud, on sõlmitud rahvusvaheline kokkulepe.

(68) „Juriidilise isiku" mõiste asutamisvabadust käsitlevate Euroopa Liidu toimimise lepingu (ELi toimimise leping) sätete kohaselt jätab ettevõtjate otsustada, millises õiguslikus vormis nad peavad sobivaks oma tegevust teostada. Seega on „juriidilised isikud" ELi toimimise lepingu tähenduses kõik isikud, kes on asutatud liikmesriigi õiguse alusel või kelle tegevus on reguleeritud liikmesriigi õigusega, sõltumata nende õiguslikust vormist.

(69) Liidu institutsioone, organeid ja asutusi innustatakse tunnustama käesoleva määrusega hõlmatud e-identimist ja usaldusteenuseid halduskoostööks, kasutades eelkõige ära olemasolevaid häid tavasid ja käimasolevate projektide tulemusi käesoleva määrusega hõlmatud valdkondades.

([1]) Komisjoni 25. veebruari 2011. aasta otsus 2011/130/EL, millega kehtestatakse pädevate asutuste poolt elektrooniliselt allkirjastatud dokumentide piiriülese töötlemise miinimumnõuded vastavalt Euroopa Parlamendi ja nõukogu direktiivile 2006/123/EÜ teenuste kohta siseturul (ELT L 53, 26.2.2011, lk 66).

(70) Käesoleva määruse teatavate tehniliste aspektide paindlikuks ja kiireks täiendamiseks peaks komisjonil olema õigus võtta kooskõlas ELi toimimise lepingu artikliga 290 vastu delegeeritud õigusakte kriteeriumide kohta, millele peavad vastama kvalifitseeritud e-allkirja andmise vahendite sertifitseerimise eest vastutavad asutused. On eriti oluline, et komisjon viiks oma ettevalmistava töö käigus läbi asjakohaseid konsultatsioone, sealhulgas ekspertide tasandil. Delegeeritud õigusaktide ettevalmistamisel ja koostamisel peaks komisjon tagama asjaomaste dokumentide sama- ja õigeaegse ning asjakohase edastamise Euroopa Parlamendile ja nõukogule.

(71) Selleks et tagada käesoleva määruse ühetaolised rakendamistingimused, tuleks komisjonile anda rakendamisvolitused eelkõige selliste standardite viitenumbrite täpsustamiseks, mille kasutamine eeldaks vastavust teatavatele käesolevas määruses sätestatud nõuetele. Neid volitusi tuleks teostada kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) nr 182/2011 ([1]).

(72) Delegeeritud õigusaktide vastuvõtmisel peaks komisjon arvesse võtma Euroopa ja rahvusvaheliste standardimisorganisatsioonide, eelkõige Euroopa Standardikomitee (CEN), Euroopa Telekommunikatsioonistandardite Instituudi (ETSI), Rahvusvahelise Standardiorganisatsiooni (ISO) ja Rahvusvahelise Telekommunikatsiooni Liidu (ITU) välja töötatud standardeid ja tehnilisi kirjeldusi, et tagada e-identimise ja usaldusteenuste turvalisuse ja koosvõime kõrge tase.

(73) Õiguskindluse ja selguse huvides tuleks direktiiv 1999/93/EÜ tunnistada kehtetuks.

(74) Selleks et tagada õiguskindlus turul osalejatele, kes juba kasutavad vastavalt direktiivile 1999/93/EÜ väljastatud kvalifitseeritud sertifikaate, on vaja ette näha piisav üleminekuaeg. Samuti tuleks ette näha üleminekumeetmed turvalise allkirja andmise vahendite jaoks, mille vastavus on kindlaks määratud direktiiviga 1999/93/EÜ, ning sertifitseerimisteenuste osutajate jaoks, kes väljastavad kvalifitseeritud sertifikaate enne 1. juulit 2016. Lisaks tuleb anda komisjoni käsutusse vahendid rakendusaktide ja delegeeritud õigusaktide vastuvõtmiseks enne nimetatud tähtaega.

(75) Käesolevas määruses sätestatud kohaldamiskuupäevad ei mõjuta liikmesriikide olemasolevaid kohustusi, mis tulenevad liidu õigusest, eelkõige direktiivist 2006/123/EÜ.

(76) Kuna käesoleva määruse eesmärke ei suuda liikmesriigid piisavalt saavutada, küll aga saab neid meetme ulatuse tõttu paremini saavutada liidu tasandil, võib liit võtta meetmeid kooskõlas Euroopa Liidu lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Kõnealuses artiklis sätestatud proportsionaalsuse põhimõtte kohaselt ei lähe käesolev määrus nimetatud eesmärkide saavutamiseks vajalikust kaugemale.

(77) Euroopa andmekaitseinspektoriga konsulteeriti kooskõlas Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 45/2001 ([2]) artikli 28 lõikega 2 ning ta esitas arvamuse 27. septembril 2012 ([3]),

([1]) Euroopa Parlamendi ja nõukogu 16. veebruari 2011. aasta määrus (EL) nr 182/2011, millega kehtestatakse eeskirjad ja üldpõhimõtted, mis käsitlevad liikmesriikide läbiviidava kontrolli mehhanisme, mida kohaldatakse komisjoni rakendamisvolituste teostamise suhtes (ELT L 55, 28.2.2011, lk 13).

([2]) Euroopa Parlamendi ja nõukogu 18. detsembri 2000. aasta määrus (EÜ) nr 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta (EÜT L 8, 12.1.2001, lk 1).

([3]) ELT C 28, 30.1.2013, lk 6.

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I PEATÜKK

ÜLDSÄTTED

Artikkel 1

Reguleerimisese

Käesolevas määruses, selleks et tagada siseturu nõuetekohane toimimine, seades samal ajal eesmärgiks saavutada e-identimise vahendite ja usaldusteenuste asjakohane turvalisuse tase:

a) sätestatakse tingimused, mille alusel peavad liikmesriigid tunnustama füüsiliste ja juriidiliste isikute e-identimise vahendeid, mis kuuluvad teise liikmesriigi teavitatud e-identimise süsteemi,

b) sätestatakse usaldusteenuste, eelkõige e-tehingute eeskirjad, ning

c) luuakse õigusraamistik e-allkirja, e-templi, e-ajatempli, e-dokumentide, registreeritud e-andmevahetusteenuste ja veebisaitide autentimise sertifitseerimisteenuste jaoks.

Artikkel 2

Kohaldamisala

1. Käesolevat määrust kohaldatakse liikmesriikide poolt teavitatud e-identimise süsteemide ja liidus asuvate usaldusteenuse osutajate suhtes.

2. Käesolevat määrust ei kohaldata selliste usaldusteenuste osutamise suhtes, mida kasutatakse eranditult suletud süsteemides, mis tulenevad siseriiklikust õigusest või määratletud osalejate kogumi vahelistest kokkulepetest.

3. Käesolev määrus ei mõjuta siseriiklikku või liidu õigust, mis reguleerib lepingute sõlmimist ja kehtivust või muude juriidiliste või menetluskohustuste tekkimist ja kehtivust seoses vorminõuetega.

Artikkel 3

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

1) „e-identimine” – protsess, mille käigus kasutatakse elektroonilisi isikutuvastusandmeid, mis tähistavad üheselt füüsilist või juriidilist isikut või juriidilist isikut esindavat füüsilist isikut;

2) „e-identimise vahend” – kehaline ja/või kehatu üksus, mis sisaldab isikutuvastusandmeid ja mida kasutatakse internetipõhiste teenuste puhul autentimiseks;

3) „isikutuvastusandmed” – andmed, mis võimaldavad teha kindlaks füüsilise või juriidilise isiku või juriidilist isikut esindava füüsilise isiku;

4) „e-identimise süsteem” – e-identimiseks vajalik süsteem, mille raames väljastatakse e-identimise vahendeid füüsilistele või juriidilistele isikutele või juriidilist isikut esindavatele füüsilistele isikutele;

5) „autentimine" – elektrooniline protsess, mis võimaldab füüsilise või juriidilise isiku e-identimist või elektrooniliste andmete päritolu ja tervikluse kinnitamist;

6) „tuginev isik" – füüsiline või juriidiline isik, kes tugineb e-identimisele või usaldusteenusele;

7) „avaliku sektori asutus" – riigi-, piirkondlik või kohalik asutus, avalik-õiguslik isik või ühe või mitme kõnealuse asutuse või avalik-õigusliku isiku poolt asutatud ühendus või eraõiguslik isik, kellele on vähemalt üks kõnealune asutus, isik või ühendus andnud õiguse osutada avalikke teenuseid, kui ta tegutseb kõnealust õigust teostades;

8) „avalik-õiguslik isik" – Euroopa Parlamendi ja nõukogu direktiivi 2014/24/EL ([1]) artikli 2 lõike 1 punktis 4 määratletud isik;

9) „allkirja andja" – e-allkirja andnud füüsiline isik;

10) „e-allkiri" – elektroonilised andmed, mis on lisatud muudele elektroonilistele andmetele või on nendega loogiliselt seotud ja mida allkirja andja kasutab allkirja andmiseks;

11) „täiustatud e-allkiri" – e-allkiri, mis vastab artiklis 26 sätestatud nõuetele;

12) „kvalifitseeritud e-allkiri" – täiustatud e-allkiri, mis antakse kvalifitseeritud e-allkirja andmise vahendi abil ja mis põhineb e-allkirja kvalifitseeritud sertifikaadil;

13) „e-allkirja andmiseks vajalikud andmed" – ainulaadsed andmed, mida allkirja andja kasutab e-allkirja andmiseks;

14) „e-allkirja sertifikaat" – elektrooniline dokument, mis seob e-allkirja valideerimise andmed füüsilise isikuga ja kinnitab vähemalt selle isiku nime või varjunime;

15) „e-allkirja kvalifitseeritud sertifikaat" – e-allkirja sertifikaat, mille väljastab kvalifitseeritud usaldusteenuse osutaja ja mis vastab I lisas sätestatud nõuetele;

16) „usaldusteenus" – elektrooniline teenus, mida tavaliselt osutatakse tasu eest ja mis seisneb:

   a) e-allkirjade, e-templite või e-ajatemplite, registreeritud e-andmevahetusteenuste ning nende teenustega seotud sertifikaatide loomises, kontrollimises ja valideerimises, või

   b) veebisaidi autentimise sertifikaatide loomises, kontrollimises ja valideerimises, või

   c) e-allkirjade, e-templite või nende teenustega seotud sertifikaatide säilitamises;

17) „kvalifitseeritud usaldusteenus" – usaldusteenus, mis vastab käesolevas määruses sätestatud kohaldatavatele nõuetele;

([1]) Euroopa Parlamendi ja nõukogu 26. veebruari 2014. aasta direktiiv 2014/24/EL, milles käsitletakse riigihankeid ja millega tunnistatakse kehtetuks direktiiv 2004/18/EÜ (ELT L 94, 28.3.2014, lk 65).

18) „vastavushindamisasutus" – määruse (EÜ) nr 765/2008 artikli 2 punktis 13 määratletud asutus, mis on kooskõlas nimetatud määrusega akrediteeritud asutusena, millel on pädevus teostada kvalifitseeritud usaldusteenuse osutaja ja tema osutatavate kvalifitseeritud usaldusteenuste vastavushindamist;

19) „usaldusteenuse osutaja" – füüsiline või juriidiline isik, kes osutab üht või mitut usaldusteenust kas kvalifitseeritud või kvalifitseerimata usaldusteenuse osutajana;

20) „kvalifitseeritud usaldusteenuse osutaja" – usaldusteenuse osutaja, kes osutab üht või mitut kvalifitseeritud usaldusteenust ning kellele järelevalveasutus on andnud kvalifitseeritud staatuse;

21) „toode" – riist- või tarkvara või riist- või tarkvara asjakohased osad, mis on ette nähtud usaldusteenuste osutamiseks;

22) „e-allkirja andmise vahend" – seadistatud tark- või riistvara, mida kasutatakse e-allkirja andmiseks;

23) „kvalifitseeritud e-allkirja andmise vahend" – e-allkirja andmise vahend, mis vastab II lisas sätestatud nõuetele;

24) „templi andja" – e-templi loonud juriidiline isik;

25) „e-tempel" – elektroonilised andmed, mis on lisatud muudele elektroonilistele andmetele või on nendega loogiliselt seotud ja mis tagavad viimatinimetatud andmete päritolu ja tervikluse;

26) „täiustatud e-tempel" – e-tempel, mis vastab artiklis 36 sätestatud nõuetele;

27) „kvalifitseeritud e-tempel" – täiustatud e-tempel, mis luuakse kvalifitseeritud e-templi loomise vahendi abil ja mis põhineb e-templi kvalifitseeritud sertifikaadil;

28) „e-templi loomiseks vajalikud andmed" – ainulaadsed andmed, mida e-templi andja kasutab e-templi loomiseks;

29) „e-templi sertifikaat" – elektrooniline dokument, mis seob e-templi valideerimise andmed juriidilise isikuga ja kinnitab selle isiku nime;

30) „e-templi kvalifitseeritud sertifikaat" – e-templi sertifikaat, mille väljastab kvalifitseeritud usaldusteenuse osutaja ja mis vastab III lisas sätestatud nõuetele;

31) „e-templi loomise vahend" – seadistatud tark- või riistvara, mida kasutatakse e-templi loomiseks;

32) „kvalifitseeritud e-templi loomise vahend" – e-templi loomise vahend, mis vastab *mutatis mutandis* II lisas sätestatud nõuetele;

33) „e-ajatempel" – elektroonilised andmed, mis seovad muud elektroonilised andmed kindla ajahetkega ja tõendavad, et viimatinimetatud andmed olid sel ajahetkel olemas;

34) „kvalifitseeritud e-ajatempel" – e-ajatempel, mis vastab artiklis 42 sätestatud nõuetele;

35) „e-dokument" – mis tahes sisu, mida säilitatakse elektroonilisel kujul, eelkõige teksti või heli visuaal- või audiovisuaalsalvestisena;

36) „registreeritud e-andmevahetusteenus" – teenus, mis võimaldab edastada kolmandate isikute vahel andmeid elektrooniliselt, tõendab edastatud andmete käitamist, sealhulgas andmete saatmist ja kättesaamist, ning kaitseb edastatud andmeid kadumise, varguse, kahjustamise või lubamatu muutmise eest;

37) „kvalifitseeritud registreeritud e-andmevahetusteenus" – registreeritud e-andmevahetusteenus, mis vastab artiklis 44 sätestatud nõuetele;

38) „sertifikaat veebisaidi autentimiseks" – dokument, mis võimaldab autentida veebisaiti ja seob selle füüsilise või juriidilise isikuga, kellele sertifikaat on väljastatud;

39) „kvalifitseeritud sertifikaat veebisaidi autentimiseks" – sertifikaat veebisaidi autentimiseks, mille on väljastanud kvalifitseeritud usaldusteenuse osutaja ja mis vastab IV lisas sätestatud nõuetele;

40) „valideerimisandmed" – andmed, mida kasutatakse e-allkirja või e-templi valideerimiseks;

41) „valideerimine" – protsess, mille käigus kontrollitakse ja kinnitatakse e-allkirja või e-templi kehtivust.

Artikkel 4

Siseturu põhimõtted

1. Liikmesriigi territooriumil ei piirata teises liikmesriigis asuva usaldusteenuse osutaja usaldusteenuste osutamist põhjustel, mis kuuluvad käesoleva määrusega hõlmatud valdkondadesse.

2. Käesoleva määrusega kooskõlas olevatel toodetel ja usaldusteenustel lubatakse siseturul vabalt ringelda.

Artikkel 5

Andmetöötlus ja -kaitse

1. Isikuandmete töödeldakse kooskõlas direktiiviga 95/46/EÜ.

2. Ilma et see piiraks siseriikliku õiguse kohast varjunimede õiguslikku toimet, ei keelata e-tehingute tegemisel varjunimede kasutamist.

II PEATÜKK

E-IDENTIMINE

Artikkel 6

Vastastikune tunnustamine

1. Kui ühes liikmesriigis nõutakse vastavalt siseriiklikule õigusele või haldustavale avaliku sektori asutuse osutatavale internetipõhisele teenusele juurdepääsuks e-identimist e-identimise vahendi abil ja e-autentimist, tunnustatakse selles liikmesriigis teises liikmesriigis väljastatud e-identimise vahendit kõnealuse internetipõhise teenuse piiriüleseks autentimiseks, kui täidetud on järgmised tingimused:

a) e-identimise vahend on väljastatud e-identimise süsteemi kohaselt, mis on kantud komisjoni poolt vastavalt artiklile 9 avaldatud nimekirja;

b) e-identimise vahendi usaldusväärsuse tase vastab usaldusväärsuse tasemele, mida avaliku sektori asutus nõuab kõnealusele internetipõhisele teenusele juurdepääsuks esimesena nimetatud liikmesriigis, või on sellest usaldusväärsuse tasemest kõrgem, eeldusel et selle e-identimise vahendi usaldusväärsuse tase on märkimisväärne või kõrge;

c) asjaomane avaliku sektori asutus kasutab kõnealusele internetipõhisele teenusele juurdepääsuks usaldusväärsuse taset, mille tase on märkimisväärne või kõrge.

Tunnustamine toimub hiljemalt 12 kuud pärast seda, kui komisjon avaldab esimese lõigu punktis a osutatud nimekirja.

2. E-identimise vahendit, mis on väljastatud komisjoni poolt vastavalt artiklile 9 avaldatud nimekirjas oleva süsteemi kohaselt ning mille usaldusväärsuse tase on madal, võivad avaliku sektori asutused tunnustada nende asutuste osutatavate internetipõhiste teenuste piiriülese autentimise eesmärgil.

Artikkel 7

E-identimise süsteemidest teavitamise tingimused

E-identimise süsteemist saab vastavalt artikli 9 lõikele 1 teavitada juhul, kui täidetud on kõik järgmised tingimused:

a) e-identimise süsteemi kuuluv e-identimise vahend on väljastatud:

i) teatava liikmesriigi poolt;

ii) teavitava liikmesriigi volituse alusel või

iii) sõltumatult teavitavast liikmesriigist ning see liikmesriik tunnustab seda;

b) e-identimise süsteemi kuuluvat e-identimise vahendit saab kasutada juurdepääsuks vähemalt ühele teenusele, mida osutab avaliku sektori asutus ja mis eeldab teavitavas liikmesriigis e-identimist;

c) e-identimise süsteem ja selle kohaselt väljastatud e-identimise vahend vastavad vähemalt ühe usaldusväärsuse taseme nõuetele, mis on sätestatud artikli 8 lõikes 3 osutatud rakendusaktis;

d) teavitav liikmesriik tagab, et ainulaadsed kõnealust isikut tähistavad isikutuvastusandmed omistatakse artikli 3 punktis 1 osutatud füüsilisele või juriidilisele isikule sellesse süsteemi kuuluva e-identimise vahendi väljastamisel kooskõlas tehniliste kirjelduste, standardite ja menetlustega, mis on artikli 8 lõikes 3 osutatud rakendusaktis ette nähtud asjakohase usaldusväärsuse taseme jaoks;

e) sellesse süsteemi kuuluvat e-identimise vahendit väljastav osaline tagab e-identimise vahendi omistamise käesoleva artikli punktis d osutatud isikule kooskõlas tehniliste kirjelduste, standardite ja menetlustega, mis on artikli 8 lõikes 3 osutatud rakendusaktis ette nähtud asjakohase usaldusväärsuse taseme jaoks;

f) teavitav liikmesriik tagab internetipõhise autentimise võimaluse nii, et teise liikmesriigi territooriumil asuv tuginev isik saab kinnitada elektrooniliselt saadud isikutuvastusandmeid.

Teavitav liikmesriik võib kindlaks määrata kõnealusee autentimise kasutustingimused tuginevatele isikutele, kes ei ole avaliku sektori asutused. Piiriülene autentimine on tasuta, kui autenditakse avaliku sektori asutuse internetipõhist teenust.

Liikmesriigid ei kehtesta autentimiskavatsusega tuginevate isikute suhtes ebaproportsionaalseid tehnilisi tingimusi, mis takistavad või raskendavad märkimisväärselt teavitatud e-identimise süsteemide koosvõimet;

g) vähemalt kuus kuud enne artikli 9 lõike 1 kohast teavitamist esitab teavitav liikmesriik teistele liikmesriikidele artikli 12 lõikest 5 tuleneva kohustuse täitmiseks selle süsteemi kirjelduse artikli 12 lõikes 7 osutatud rakendusaktidega kehtestatud menetluskorra kohaselt;

h) e-identimise süsteem vastab artikli 12 lõikes 8 osutatud rakendusaktis sätestatud nõuetele.

Artikkel 8

E-identimise süsteemide usaldusväärsuse tasemed

1. E-identimise süsteemis, millest on teavitatud artikli 9 lõike 1 kohaselt, määratakse süsteemi raames väljastatud e-identimise vahenditele madal, märkimisväärne ja/või kõrge usaldusväärsuse tase.

2. Madal, märkimisväärne ja kõrge usaldusväärsuse tase vastab järgmistele nõuetele:

a) madal usaldusväärsuse tase osutab e-identimise süsteemi kuuluvale e-identimise vahendile, mis on isiku väidetava või tema poolt kinnitatud isikusamasuse tuvastamiseks piiratud määral usaldusväärne ning mille kirjeldamisel osutatakse sellega seotud tehnilistele kirjeldustele, standarditele ja menetlustele, sealhulgas tehnilisele kontrollile, mille eesmärk on vähendada isikuandmete väärkasutamise või muutmise ohtu;

b) märkimisväärne usaldusväärsuse tase osutab e-identimise süsteemi kuuluvale e-identimise vahendile, mis on isiku väidetava või tema poolt kinnitatud isikusamasuse tuvastamiseks olulisel määral usaldusväärne ning mille kirjeldamisel osutatakse sellega seotud tehnilistele kirjeldustele, standarditele ja menetlustele, sealhulgas tehnilisele kontrollile, mille eesmärk on vähendada märkimisväärselt isikuandmete väärkasutamise või muutmise ohtu;

c) kõrge usaldusväärsuse tase osutab e-identimise süsteemi kuuluvale e-identimise vahendile, mis on isiku väidetava või tema poolt kinnitatud isikusamasuse tuvastamiseks kõrgema usaldusväärsuse tasemega kui märkimisväärse usaldusväärsuse tasemega e-identimise vahend ning mille kirjeldamisel osutatakse sellega seotud tehnilistele kirjeldustele, standarditele ja menetlustele, sealhulgas tehnilisele kontrollile, mille eesmärk on hoida ära isikuandmete väärkasutamist või muutmist.

3. Võttes arvesse asjakohaseid rahvusvahelisi standardeid ja vastavalt lõikele 2 kehtestab komisjon hiljemalt 18. septembriks 2015 rakendusaktidega minimaalsed tehnilised kirjeldused, standardid ja menetlused, mille suhtes määratakse lõike 1 kohaldamise eesmärgil e-identimise vahendite jaoks kindlaks madal, märkimisväärne või kõrge usaldusväärsuse tase.

Nimetatud minimaalsed tehnilised kirjeldused, standardid ja menetlused kehtestatakse, kasutades lähtealusena järgmiste elementide usaldusväärsust ja kvaliteeti:

a) e-identimise vahendi väljastamist taotleva füüsilise või juriidilise isiku isikusamasuse tõendamise ja kontrollimise menetlus;

b) taotletava e-identimise vahendi väljastamise menetlus;

c) autentimise mehhanism, kus füüsiline või juriidiline isik kasutab e-identimise vahendit selleks, et kinnitada oma isikusamasust tuginevale isikule;

d) e-identimise vahendit väljastav üksus;

e) muu asutus, kes osaleb e-identimise vahendi väljastamise taotlemises, ning

f) väljastatud e-identimise vahendite tehnilised kirjeldused ja turvaspetsifikaadid.

Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 9

Teavitamine

1. Teavitav liikmesriik edastab komisjonile järgmise teabe ja põhjendamatu viivituseta selle iga hilisema muudatuse:

a) e-identimise süsteemi kirjeldus. kaasa arvatud selle usaldusväärsuse tase ja sellesse süsteemi kuuluvate e-identimise vahendite väljastaja(d);

b) kohaldatav järelevalvekord ja järgmine vastutuskorda puudutav teave:

i) e-identimise vahendit väljastav osaline ning

ii) autentimismenetlust läbiviiv osaline;

c) teavitatud e-identimise süsteemi eest vastutav asutus või vastutavad asutused;

d) teave ainulaadsete isikutuvastusandmete registreerimist haldava üksuse või haldavate üksuste kohta;

e) kirjeldus, kuidas täidetakse artikli 12 lõikes 8 osutatud rakendusaktis sätestatud nõuded;

f) artikli 7 punktis f osutatud autentimise kirjeldus;

g) teavitatud e-identimise süsteemi, autentimise või asjaomase ohustatud osa peatamise või tühistamise kord.

2. Üks aasta pärast artikli 8 lõikes 3 ja artikli 12 lõikes 8 osutatud rakendusaktide kohaldamise alguskuupäeva avaldab komisjon *Euroopa Liidu Teatajas* nimekirja e-identimise süsteemidest, millest on teavitatud vastavalt käesoleva artikli lõikele 1, ja nendega seotud põhiteabe.

3. Kui komisjoni teavitatakse pärast lõikes 2 osutatud ajavahemiku möödumist, avaldab ta *Euroopa Liidu Teatajas* lõikes 2 osutatud nimekirja muudatused kahe kuu jooksul alates kõnealuse teate saamise kuupäevast.

4. Liikmesriik võib komisjonile esitada taotluse jätta selle liikmesriigi poolt teavitatud e-identimise süsteem lõikes 2 osutatud nimekirjast välja. Komisjon avaldab vastavad nimekirja muudatused *Euroopa Liidu Teatajas* ühe kuu jooksul pärast liikmesriigilt taotluse saamist.

5. Komisjon võib rakendusaktidega kindlaks määrata lõikes 1 osutatud teavitamise asjaolud, formaadid ja menetlused. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 10

Turvarikkumine

1. Kui artikli 9 lõike 1 kohaselt teavitatud e-identimise süsteemi või artikli 7 punktis f osutatud autentimist rikutakse või see on osaliselt ohustatud viisil, mis mõjutab selle süsteemi piiriülese autentimise usaldusväärsust, peatab või tühistab teavitav liikmesriik viivitamata selle piiriülese autentimise või asjaomaste ohustatud osade toimimise ning teavitab sellest teisi liikmesriike ja komisjoni.

2. Pärast lõikes 1 osutatud rikkumise või ohu kõrvaldamist taastab teavitav liikmesriik piiriülese autentimise ning teavitab sellest ilma põhjendamatu viivituseta teisi liikmesriike ja komisjoni.

3. Kui lõikes 1 osutatud rikkumist või ohtu ei kõrvaldata kolme kuu jooksul alates peatamisest või tühistamisest, teatab teavitav liikmesriik e-identimise süsteemi kasutamise lõpetamisest teistele liikmesriikidele ja komisjonile.

Komisjon avaldab põhjendamatu viivituseta *Euroopa Liidu Teatajas* artikli 9 lõikes 2 osutatud nimekirjas tehtud muudatused.

Artikkel 11

Vastutus

1. Teavitav liikmesriik vastutab füüsilisele või juriidilisele isikule tahtlikult või ettevaatamatusest tekitatud kahju eest, mis tuleneb artikli 7 punktides d ja f sätestatud kohustuste täitmata jätmisest piiriüleses tehingus.

2. E-identimise vahendit väljastav osaline vastutab füüsilisele või juriidilisele isikule tahtlikult või ettevaatamatusest tekitatud kahju eest, mis tuleneb artikli 7 punktis e sätestatud kohustuste täitmata jätmisest piiriüleses tehingus.

3. Autentimismenetlust läbiviiv osaline vastutab füüsilisele või juriidilisele isikule tahtlikult või ettevaatamatusest tekitatud kahju eest, mis tuleneb artikli 7 punktis f sätestatud autentimise nõuetekohase toimimise tagamata jätmisest piiriüleses tehingus.

4. Lõikeid 1, 2 ja 3 kohaldatakse kooskõlas siseriiklike vastutust käsitlevate eeskirjadega.

5. Lõiked 1, 2 ja 3 ei piira osaliste siseriikliku õiguse kohast vastutust tehingutes, milles kasutatakse artikli 9 lõike 1 kohaselt teavitatud e-identimise süsteemi kuuluvaid e-identimise vahendeid.

Artikkel 12

Koostöö ja koosvõime

1. Artikli 9 lõike 1 kohaselt teavitatud riiklikud e-identimise süsteemid peavad olema koosvõimelised.

2. Lõike 1 kohaldamise eesmärgil luuakse koosvõime raamistik.

3. Koosvõime raamistik peab vastama järgmistele nõuetele:

a) see on tehnoloogiliselt neutraalne ja ei diskrimineeri asjaomases liikmesriigis ühtegi konkreetset siseriiklikku e-identimise tehnilist lahendust;

b) see vastab võimaluse korral Euroopa ja rahvusvahelistele standarditele;

c) see hõlbustab lõimitud eraelukaitse põhimõtte rakendamist ning

d) see tagab isikuandmete töötlemise kooskõlas direktiiviga 95/46/EÜ.

4. Koosvõime raamistik koosneb järgmisest:

a) viide artiklis 8 sätestatud usaldusväärsuse tasemetega seotud tehnilistele miinimumnõuetele;

b) teavitatud e-identimise süsteemide siseriiklike usaldusväärsuse tasemete seostamine artikli 8 kohaste usaldusväärsuse tasemetega;

c) viide ette nähtud tehnilise koosvõime miinimumnõuetele;

d) viide e-identimise süsteemidest kättesaadavatele minimaalsele hulgale isikutuvastamisandmetele, mis tähistavad ainuüksi üht füüsilist või juriidilist isikut;

e) menetluseeskirjad;

f) vaidluste lahendamise kord ning

g) ühised toimimise turvalisuse standardid.

5. Liikmesriigid teevad koostööd seoses järgmisega:

a) koosvõime artikli 9 lõike 1 kohaselt teavitatud e-identimise süsteemide ja nende e-identimise süsteemide vahel, millest liikmesriigid kavatsevad teavitada, ning

b) e-identimise süsteemide turvalisus.

6. Liikmesriikide vaheline koostöö hõlmab järgmist:

a) teabe, kogemuste ja heade tavade vahetamine e-identimise süsteemide ning eelkõige koosvõime ja usaldusväärsuse tasemetega seotud tehniliste nõuete kohta;

b) teabe, kogemuste ja heade tavade vahetamine artiklis 8 sätestatud e-identimise süsteemide usaldusväärsuse tasemetega töötamise kohta;

c) käesoleva määruse kohaldamisalasse kuuluvate e-identimise süsteemide vastastikune hindamine ning

d) e-identimise sektoris toimuvate asjakohaste arengute analüüsimine.

7. Komisjon kehtestab hiljemalt 18. märtsiks 2015 rakendusaktidega vajaliku menetluskorra lõigetes 5 ja 6 osutatud liikmesriikidevahelise koostöö hõlbustamiseks, et edendada usalduse ja turvalisuse kõrget taset, mis vastab riski astmele.

8. Selleks et näha ette ühtsed tingimused lõikest 1 tuleneva nõude rakendamiseks, võtab komisjon hiljemalt 18. septembriks 2015 lõikes 3 sätestatud kriteeriumite kohaselt ja liikmesriikidevahelise koostöö tulemusi arvesse võttes vastu rakendusaktid lõikes 4 sätestatud koosvõime raamistiku kohta.

9. Käesoleva artikli lõigetes 7 ja 8 osutatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

III PEATÜKK

USALDUSTEENUSED

1. JAGU

Üldsätted

Artikkel 13

Vastutus ja tõendamiskoormis

1. Ilma et see piiraks lõike 2 kohaldamist, vastutavad usaldusteenuse osutajad füüsilisele või juriidilisele isikule tahtlikult või ettevaatamatusest tekitatud kahju eest, mis tuleneb käesolevas määruses sätestatud kohustuste täitmata jätmisest.

Kvalifitseerimata usaldusteenuse osutaja tegevuse tahtlikkuse või ettevaatamatuse tõendamise kohustus lasub füüsilisel või juriidilisel isikul, kes väidab, et talle on põhjustatud esimeses lõigus osutatud kahju.

Eeldatakse, et kvalifitseeritud usaldusteenuse osutaja on tegutsenud tahtlikult või ettevaatamatusest, kui nimetatud kvalifitseeritud usaldusteenuse osutaja ei tõesta, et esimeses lõigus osutatud kahju põhjustati ilma selle kvalifitseeritud usaldusteenuse osutaja tahtliku või ettevaatamatu tegutsemiseta.

2. Kui usaldusteenuse osutajad teavitavad oma kliente eelnevalt nõuetekohaselt nende poolt osutatavate teenuste kasutamise piirangutest ja need piirangud on kolmandatele isikutele arusaadavad, siis ei vastuta usaldusteenuse osutajad kahju eest, mis tuleneb osutatud piiranguid ületavast teenuste kasutamisest.

3. Lõikeid 1 ja 2 kohaldatakse kooskõlas siseriiklike vastutust käsitlevate eeskirjadega.

Artikkel 14

Rahvusvahelised aspektid

1. Kolmandas riigis asuvate usaldusteenuse osutajate pakutavad usaldusteenused tunnistatakse õiguslikult samaväärseteks liidu territooriumil asuvate kvalifitseeritud usaldusteenuse osutajate pakutavate kvalifitseeritud usaldusteenustega juhul, kui kolmandast riigist pärit usaldusteenuseid tunnustatakse liidu ja kõnealuse kolmanda riigi või rahvusvahelise organisatsiooni vahel sõlmitud kokkuleppe alusel kooskõlas ELi toimimise lepingu artikliga 218.

2. Lõikes 1 osutatud kokkulepetega tagatakse eelkõige, et:

a) kolmanda riigi usaldusteenuse osutajad või rahvusvahelised organisatsioonid, kellega on sõlmitud kokkulepe, ning nende osutatavad teenused vastavad liidus asuvate kvalifitseeritud usaldusteenuse osutajate ja nende osutatavate kvalifitseeritud usaldusteenuste suhtes kohaldatavatele nõuetele;

b) liidus asuvate kvalifitseeritud usaldusteenuse osutajate poolt osutatavad kvalifitseeritud usaldusteenused tunnistatakse õiguslikult samaväärseteks usaldusteenustega, mida osutavad kolmandas riigis asuvad usaldusteenuse osutajad või rahvusvahelised organisatsioonid, kellega on sõlmitud kokkulepe.

Artikkel 15

Puuetega inimeste takistusteta juurdepääs

Kui see on teostatav, tuleks osutatavad usaldusteenused ja kõnealuste teenuste osutamisel kasutatavad lõpptarbijale suunatud tooted teha puuetega inimestele juurdepääsetavaks.

Artikkel 16

Karistused

Liikmesriigid kehtestavad eeskirjad käesoleva määruse rikkumise eest kohaldatavate karistuste kohta. Kehtestatud karistused peavad olema tõhusad, proportsionaalsed ja hoiatavad.

2. JAGU

Järelevalve

Artikkel 17

Järelevalveasutus

1. Liikmesriigid määravad järelevalveasutuse, mis asub nende territooriumil või, vastastikusel kokkuleppel teise liikmesriigiga, kõnealuses teises liikmesriigis asuva järelevalveasutuse. Nimetatud asutus vastutab määravas liikmesriigis järelevalveülesannete täitmise eest.

Järelevalveasutustele antakse nende ülesannete täitmiseks vajalikud volitused ja piisavad vahendid.

2. Liikmesriigid teatavad komisjonile enda poolt määratud järelevalveasutuste nimed ja aadressid.

3. Järelevalveasutuse ülesandeks on:

a) teostada eelneva ja järgneva järelevalve käigus määrava liikmesriigi territooriumil asuvate kvalifitseeritud usaldusteenuse osutajate üle järelevalvet selle tagamiseks, et kvalifitseeritud usaldusteenuse osutajad ja nende osutatavad kvalifitseeritud usaldusteenused vastaksid käesolevas määruses sätestatud nõuetele;

b) võtta järgneva järelevalve käigus vajaduse korral meetmeid määrava liikmesriigi territooriumil asuvate kvalifitseerimata usaldusteenuse osutajate suhtes, kui järelevalveasutusele teatatakse, et kvalifitseerimata usaldusteenuse osutajad või nende osutatavad usaldusteenused ei vasta väidetavalt käesolevas määruses sätestatud nõuetele.

4. Lõike 3 kohaldamisel ja tulenevalt selles sätestatud piirangutest on järelevalveasutuse ülesanne eelkõige:

a) teha koostööd teiste järelevalveasutustega ja anda neile abi kooskõlas artikliga 18;

b) analüüsida artikli 20 lõikes 1 ja artikli 21 lõikes 1 osutatud vastavushindamisaruandeid;

c) teavitada teisi järelevalveasutusi ja üldsust turvarikkumistest ja tervikluse kaost kooskõlas artikli 19 lõikega 2;

d) anda komisjonile aru oma põhitegevusest kooskõlas käesoleva artikli lõikega 6;

e) korraldada auditeid või paluda vastavushindamisasutusel teostada kvalifitseeritud usaldusteenuse osutajate vastavushindamine kooskõlas artikli 20 lõikega 2;

f) teha andmekaitseasutustega koostööd, eelkõige teavitades neid põhjendamatu viivituseta kvalifitseeritud usaldusteenuse osutajate auditite tulemustest, kui näib, et isikuandmete kaitse eeskirju on rikutud;

g) anda usaldusteenuse osutajatele ja nende osutatavatele teenustele kvalifitseeritud staatus ning võtta see staatus ära kooskõlas artiklitega 20 ja 21;

h) teavitada artikli 22 lõikes 3 osutatud riigisiseste usaldusnimekirjade eest vastutavat asutust oma otsustest anda kvalifitseeritud staatus või võtta see ära, välja arvatud juhul, kui kõnealune asutus on samuti järelevalveasutus;

i) kontrollida lõpetamiskava käsitlevate sätete olemasolu ja nõuetekohast kohaldamist juhtudel, kui kvalifitseeritud usaldusteenuse osutajad lõpetavad oma tegevuse, sealhulgas seda, kuidas teave hoitakse kättesaadavana kooskõlas artikli 24 lõike 2 punktiga h;

j) nõuda usaldusteenuse osutajatelt käesolevas määruses sätestatud nõuete täitmata jätmise heastamist.

5. Liikmesriigid võivad nõuda, et järelevalveasutus looks, haldaks ja ajakohastaks usaldusteenuste infrastruktuuri kooskõlas siseriiklikus õiguses sätestatud tingimustega.

6. Iga järelevalveasutus esitab igal aastal 31. märtsiks komisjonile aruande oma eelmise kalendriaasta põhitegevuse kohta ning kokkuvõtte usaldusteenuse osutajatelt artikli 19 lõike 2 kohaselt saadud rikkumisteadetest.

7. Komisjon teeb lõikes 6 osutatud aastaaruande liikmesriikidele kättesaadavaks.

8. Komisjon võib rakendusaktidega määrata kindlaks lõikes 6 osutatud aruande formaadid ja menetlused. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 18

Vastastikune abi

1. Järelevalveasutused teevad koostööd heade tavade vahetamiseks.

Järelevalveasutus annab teiselt järelevalveasutuselt saadud põhjendatud taotluse korral kõnealusele asutusele abi, et järelevalveasutuste tegevus saaks toimuda järjepidevalt. Vastastikune abi võib hõlmata eelkõige teabenõudeid ja järelevalvemeetmeid, näiteks taotlusi artiklites 20 ja 21 osutatud vastavushindamisaruannetega seotud kontrollide läbiviimiseks.

2. Järelevalveasutus, kellele abitaotlus on adresseeritud, võib taotluse täitmisest keelduda mis tahes järgmisel alusel:

a) järelevalveasutus ei ole pädev taotletavat abi andma;

b) taotletav abi ei ole proportsionaalne järelevalveasutuse poolt kooskõlas artikliga 17 teostatava järelevalvega;

c) taotletava abi andmine oleks vastuolus käesoleva määrusega.

3. Kui see on asjakohane, võivad liikmesriigid anda oma vastavatele järelevalveasutustele volitused korraldada ühiseid uurimisi, millesse on kaasatud teiste liikmesriikide järelevalveasutuste töötajad. Asjaomased liikmesriigid lepivad kokku sellise ühistegevuse korra ja protseduurid ning kehtestavad need oma riigi õiguse kohaselt.

Artikkel 19

Usaldusteenuse osutajate suhtes kohaldatavad turvanõuded

1. Kvalifitseeritud ja kvalifitseerimata usaldusteenuse osutajad võtavad asjakohased tehnilised ja korralduslikud meetmed, et ohjata nende osutatavate usaldusteenuste turvalisusega seotud riske. Tehnoloogia viimaseid arenguid arvesse võttes tagatakse nende meetmetega riski astmele vastav turvalisuse tase. Eelkõige võetakse meetmeid turvaintsidentide vältimiseks ja nende mõju minimeerimiseks ning sidusrühmade teavitamiseks intsidentide kahjulikust mõjust.

2. Kvalifitseeritud ja kvalifitseerimata usaldusteenuse osutajad teavitavad järelevalveasutust ning vajaduse korral teisi asjakohaseid asutusi, nagu infoturbe eest vastutav pädev riiklik asutus või andmekaitseasutus, igast turvarikkumisest või tervikluse kaost, millel on märkimisväärne mõju osutatavale usaldusteenusele või selles sisalduvatele isikuandmetele, tehes seda põhjendamatu viivituseta, ent igal juhul 24 tunni jooksul pärast sellest teadasaamist.

Kui turvarikkumisel või tervikluse kaol on tõenäoliselt kahjulik mõju füüsilisele või juriidilisele isikule, kellele usaldusteenus on osutatud, teavitab usaldusteenuse osutaja põhjendamatu viivituseta ka füüsilist või juriidilist isikut turvarikkumisest või tervikluse kaost.

Kui see on asjakohane ja eelkõige juhul, kui turvarikkumine või tervikluse kadu hõlmab kahte või enamat liikmesriiki, teavitab teavitatud järelevalveasutus teiste asjaomaste liikmesriikide järelevalveasutusi ning ENISA-t.

Kui teavitatud järelevalveasutus leiab, et turvarikkumise või tervikluse kao avalikustamine on avalikes huvides, teavitab ta üldsust või nõuab üldsuse teavitamist asjaomaselt usaldusteenuse osutajalt.

3. Järelevalveasutus esitab ENISA-le kord aastas kokkuvõtte usaldusteenuse osutajatelt saadud turvarikkumise või tervikluse kao teadetest.

4. Komisjon võib rakendusaktidega:

a) täpsustada lähemalt lõikes 1 osutatud meetmeid ning

b) määrata kindlaks lõike 2 kohaldamisega seotud formaadid ja menetlused, sealhulgas tähtajad.

Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

3. JAGU

Kvalifitseeritud usaldusteenus

Artikkel 20

Kvalifitseeritud usaldusteenuse osutajate järelevalve

1. Vastavushindamisasutus auditeerib kvalifitseeritud usaldusteenuse osutajaid nende oma kulul vähemalt iga 24 kuu järel. Auditi eesmärk on saada kinnitust, et kvalifitseeritud usaldusteenuse osutajad ja nende osutatavad kvalifitseeritud usaldusteenused vastavad käesolevas määruses sätestatud nõuetele. Kvalifitseeritud usaldusteenuse osutaja esitavad vastavushindamisaruande järelevalveasutusele kolme tööpäeva pikkuse jooksul alates selle saamisest.

2. Ilma et see piiraks lõike 1 kohaldamist, võib järelevalveasutus kvalifitseeritud usaldusteenuse osutajaid igal ajal auditeerida või nõuda, et vastavushindamisasutus teostaks kvalifitseeritud usaldusteenuse osutajate vastavushindamise nende kvalifitseeritud usaldusteenuse osutajate kulul kinnituse saamiseks, et kõnealused kvalifitseeritud usaldusteenuse osutajad ja nende osutatavad kvalifitseeritud usaldusteenused vastavad käesolevas määruses sätestatud nõuetele. Kui isikuandmete kaitse eeskirju on ilmselt rikutud, teavitab järelevalveasutus auditite tulemustest andmekaitseasutusi.

3. Kui järelevalveasutus nõuab, et kvalifitseeritud usaldusteenuse osutaja heastaks käesolevas määruses sätestatud nõuete täitmata jätmise, kuid asjaomane teenuseosutaja ei tee seda, ning järelevalveasutuse seatud ajavahemiku jooksul (kui see on kohaldatav), võib järelevalveasutus eelkõige asjaomase rikkumise ulatust, kestust ja tagajärgi arvestades võtta sellelt teenuseosutajalt või tema osutatavalt asjaomaselt teenuselt kvalifitseeritud staatuse ning teavitada artikli 22 lõikes 3 osutatud asutust artikli 22 lõikes 1 osutatud usaldusnimekirjade ajakohastamise eesmärgil. Järelevalveasutus teavitab kvalifitseeritud usaldusteenuse osutajat temalt kvalifitseeritud staatuse või asjaomaselt teenuselt kvalifitseeritud staatuse äravõtmisest.

4. Komisjon võib rakendusaktidega kehtestada järgmiste standardite viitenumbri:

a) standardid vastavushindamisasutuste akrediteerimise ja lõikes 1 osutatud vastavushindamisaruande jaoks;

b) standardid auditeerimiseeskirjade kohta, mille alusel vastavushindamisasutused hindavad kvalifitseeritud usaldusteenuse osutajate nõuetele vastavust, nagu on osutatud lõikes 1.

Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 21

Kvalifitseeritud usaldusteenuse osutamise alustamine

1. Kui usaldusteenuse osutajad, kellel ei ole kvalifitseeritud staatust, kavatsevad alustada kvalifitseeritud usaldusteenuse osutamist, esitavad nad järelevalveasutusele teate oma kavatsusest ja vastavushindamisasutuse koostatud vastavushindamisaruande.

2. Järelevalveasutus kontrollib usaldusteenuse osutaja ja tema osutatavate usaldusteenuste vastavust käesolevas määruses sätestatud nõuetele ning eelkõige kvalifitseeritud usaldusteenuse osutajatele ja nende osutatavatele kvalifitseeritud usaldusteenustele ette nähtud nõuetele.

Kui järelevalveasutus leiab, et usaldusteenuse osutaja ja tema osutatavad teenused vastavad esimeses lõigus osutatud nõuetele, annab järelevalveasutus usaldusteenuse osutajale ja tema osutatavatele usaldusteenustele kvalifitseeritud staatuse ning teavitab artikli 22 lõikes 3 osutatud asutust artikli 22 lõikes 1 osutatud usaldusnimekirjade ajakohastamise eesmärgil hiljemalt kolm kuud pärast käesoleva artikli lõike 1 kohast teavitamist.

Kui kontrolli ei ole kolme kuu jooksul alates teavitamisest lõpule viidud, teavitab järelevalveasutus usaldusteenuse osutajat viivituse põhjustest ja ajavahemikust, mille jooksul kontroll lõpule viiakse.

3. Kvalifitseeritud usaldusteenuse osutaja võib alustada kvalifitseeritud usaldusteenuse osutamist, kui kvalifitseeritud staatus on kantud artikli 22 lõikes 1 osutatud usaldusnimekirjadesse.

4. Komisjon võib rakendusaktidega kindlaks määrata lõigete 1 ja 2 kohaldamisega seotud formaadid ja menetlused. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 22

Usaldusnimekirjad

1. Iga liikmesriik koostab, haldab ja avaldab usaldusnimekirju, mis sisaldavad teavet tema vastutusalasse kuuluvate kvalifitseeritud usaldusteenuse osutajate ja nende osutatavate kvalifitseeritud usaldusteenuste kohta.

2. Liikmesriigid koostavad elektrooniliselt allkirjastatud või e-templiga varustatud, lõikes 1 osutatud usaldusnimekirjad, haldavad neid ja avaldavad need turvalisel viisil ja automaatseks töötlemiseks sobivas formaadis.

3. Liikmesriigid edastavad komisjonile põhjendamatu viivituseta teabe, mis hõlmab riigisiseste usaldusnimekirjade koostamise, haldamise ja avaldamise eest vastutavat asutust, kõnealuste nimekirjade avaldamise koha üksikasju, nimekirjade allkirjastamiseks või templiga varustamiseks kasutatavaid sertifikaate ning nimekirjade mis tahes muudatusi.

4. Komisjon teeb lõikes 3 osutatud teabe turvalise kanali kaudu avalikkusele kättesaadavaks automaatseks töötlemiseks sobivas, elektrooniliselt allkirjastatud või e-templiga varustatud formaadis.

5. Komisjon täpsustab hiljemalt 18. septembriks 2015 rakendusaktidega lõikes 1 osutatud teabe ning määrab kindlaks lõigete 1–4 kohaldamisega seotud usaldusnimekirjade tehnilised kirjeldused ja formaadid. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 23

ELi kvalifitseeritud usaldusteenuse usaldusmärk

1. Pärast artikli 21 lõike 2 teises lõigus osutatud kvalifitseeritud staatuse märkimist artikli 22 lõikes 1 osutatud usaldusnimekirjadesse võivad kvalifitseeritud usaldusteenuse osutajad kasutada ELi usaldusmärki nende osutatavate kvalifitseeritud usaldusteenuste esitamiseks lihtsalt, äratuntavalt ja selgelt.

2. Lõikes 1 osutatud ELi kvalifitseeritud usaldusteenuse usaldusmärgi kasutamisel tagavad kvalifitseeritud usaldusteenuse osutajad asjaomasele usaldusnimekirjale viitava lingi avaldamise oma veebisaidil.

3. 1. juuliks 2015 näeb komisjon rakendusaktidega ette ELi kvalifitseeritud usaldusteenuse usaldusmärgi formaadi ja eelkõige märgi esitusviisi, koostisosade, suuruse ja kujunduse kirjelduse. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 24

Nõuded kvalifitseeritud usaldusteenuse osutajatele

1. Usaldusteenusele kvalifitseeritud sertifikaati väljastades kontrollib kvalifitseeritud usaldusteenuse osutaja asjakohaste vahenditega ja siseriikliku õiguse kohaselt selle füüsilise või juriidilise isiku identiteeti, kellele kvalifitseeritud sertifikaat väljastatakse, ja vajaduse korral tema eritunnuseid.

Kvalifitseeritud usaldusteenuse osutaja kontrollib esimeses lõigus osutatud teavet siseriikliku õiguse kohaselt kas otse või kolmandale isikule tuginedes. Kontrollimine toimub ühel järgmisel moel:

a) füüsilise isiku või juriidilise isiku volitatud esindaja füüsilise kohaloleku alusel või

b) kaughindamise teel, kasutades e-identimise vahendeid, mille puhul enne kvalifitseeritud sertifikaadi väljastamist tagati füüsilise isiku või juriidilise isiku volitatud esindaja füüsiline kohalolek ja mis vastavad artiklis 8 kehtestatud nõuetele seoses märkimisväärse või kõrge usaldusväärsuse tasemega, või

c) kooskõlas punktiga a või b väljastatud kvalifitseeritud e-allkirja või kvalifitseeritud e-templi sertifikaadi abil või

d) kasutades muid riiklikul tasandil tunnustatud identimismeetodeid, mis tagavad füüsilise kohalolekuga samaväärse usaldusväärsuse. Nimetatud samaväärne usaldusväärsus peab olema vastavushindamisasutuse poolt kinnitatud.

2. Kvalifitseeritud usaldusteenuseid osutav kvalifitseeritud usaldusteenuse osutaja:

a) teavitab järelevalveasutust muutusest oma kvalifitseeritud usaldusteenuste osutamises ja kavatsusest kõnealune tegevus lõpetada;

b) võtab tööle personali ja vajaduse korral alltöövõtjad, kellel on vajalik pädevus, usaldusväärsus, kogemus ja kvalifikatsioon ning kes on saanud turva- ja isikuandmete kaitse eeskirjade alal asjakohase koolituse ja rakendavad Euroopa või rahvusvahelistele standarditele vastavaid haldus- ja juhtimismenetlusi;

c) seoses artikli 13 kohase vastutusega võimalike kahjude eest omab piisavat hulka rahalisi vahendeid ja/või sõlmib asjakohase vastutuskindlustuse kooskõlas siseriikliku õigusega;

d) teavitab enne lepingu sõlmimist kõiki kvalifitseeritud usaldusteenust kasutada soovivaid isikuid selgelt ja põhjalikult kõnealuse teenuse kasutamise täpsetest tingimustest, sealhulgas kõigist selle kasutamise piirangutest;

e) kasutab usaldusväärseid süsteeme ja tooteid, mis on kaitstud muutmise eest, ja tagab nende toetatavate toimingute tehnilise turvalisuse ja usaldusväärsuse;

f) kasutab usaldusväärseid süsteeme talle esitatud andmete säilitamiseks ehtsuse tõendamist võimaldavas formaadis nii, et:

i) need on otsingutes avalikult kättesaadavad üksnes siis, kui isik, kellega andmed on seotud, on andnud selleks nõusoleku,

ii) säilitatud andmeid saavad sisestada ja muuta üksnes selleks volitatud isikud,

iii) on võimalik kindlaks teha, kas andmed on ehtsad;

g) võtab asjakohaseid meetmeid andmete võltsimise ja varguse vastu;

h) salvestab ja hoiavad kättesaadavana sobiva tähtaja jooksul, sealhulgas pärast seda, kui kvalifitseeritud usaldusteenuse osutaja on tegevuse lõpetanud, kogu asjakohase teabe kvalifitseeritud usaldusteenuse osutaja väljastatud ja saadud andmete kohta, eelkõige tõendina kasutamiseks kohtumenetlustes ja selleks, et tagada teenuse järjepidevus. Sellised andmed võib salvestada elektrooniliselt;

i) omab teenuse järjepidevuse tagamiseks ajakohast tegevuse lõpetamise kava, mis vastab järelevalveasutuse poolt artikli 17 lõike 4 punkti i kohaselt kontrollitud sätetele;

j) tagab isikuandmete seadusliku töötlemise vastavalt direktiivile 95/46/EÜ;

k) juhul kui kvalifitseeritud usaldusteenuse osutaja väljastab kvalifitseeritud sertifikaate, loob sertifikaatide andmebaasi ja ajakohastab seda.

3. Kui kvalifitseeritud sertifikaate väljastav kvalifitseeritud usaldusteenuse osutaja otsustab sertifikaadi tühistada, registreerib ta tühistamise oma sertifikaatide andmebaasis ning avaldab sertifikaadi tühistatud staatuse aegsasti, ning igal juhul 24 tunni jooksul pärast vastava taotluse saamist. Tühistamine jõustub kohe pärast selle avaldamist.

4. Seoses lõikega 3 annavad kvalifitseeritud sertifikaate väljastavad kvalifitseeritud usaldusteenuse osutajad tuginevatele isikutele teavet nende väljastatud kvalifitseeritud sertifikaatide kehtivus- või tühistamisstaatuse kohta. Kõnealune teave tehakse igal ajal ning pärast sertifikaadi kehtivusaja lõppu vähemalt iga sertifikaadi kohta eraldi kättesaadavaks automaatsel viisil, mis on usaldusväärne, tasuta ja tõhus.

5. Komisjon võib rakendusaktidega kehtestada käesoleva artikli lõike 2 punktides e ja f esitatud nõuetele vastavate usaldusväärsete süsteemide ja toodete standardite viitenumbrid. Kui usaldusväärsed süsteemid ja tooted vastavad kõnealustele standarditele, loetakse need käesolevas artiklis sätestatud nõuetele vastavaks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

4. JAGU

E-allkirjad

Artikkel 25

E-allkirjade õiguslik toime

1. E-allkirja ei tunnistata õiguslikult kehtetuks ega kohtumenetlustes tõenduskõlbmatuks ainuüksi seetõttu, et see on elektroonilisel kujul või ei vasta kvalifitseeritud e-allkirjadele esitatavatele nõuetele.

2. Kvalifitseeritud e-allkirjal on käsitsi kirjutatud allkirjaga samaväärne õiguslik toime.

3. Ühes liikmesriigis väljastatud kvalifitseeritud sertifikaadil põhinevat kvalifitseeritud e-allkirja tunnustatakse kvalifitseeritud e-allkirjana ka kõikides teistes liikmesriikides.

Artikkel 26

Nõuded täiustatud e-allkirjale

Täiustatud e-allkiri vastab järgmistele nõuetele:

a) see on seotud ainuüksi allkirja andjaga;

b) selle abil on võimalik allkirja andjat tuvastada;

c) see antakse e-allkirja andmiseks vajalike andmete abil, mida saab kõrge salastatuse taseme juures kasutada üksnes allkirja andja, ning

d) see on allkirjastatud andmetega seotud sellisel viisil, et kõik hilisemad andmete muudatused on tuvastatavad.

Artikkel 27

E-allkirjad avalikus teenistuses

1. Kui liikmesriik nõuab avaliku sektori asutuse poolt või tema nimel osutatava internetipõhise teenuse kasutamiseks täiustatud e-allkirja, tunnustab see liikmesriik täiustatud e-allkirju, e-allkirja kvalifitseeritud sertifikaadil põhinevaid täiustatud e-allkirju ja kvalifitseeritud e-allkirju, mis on antud vähemalt lõikes 5 osutatud formaadis või rakendusaktides määratletud meetodeid kasutades.

2. Kui liikmesriik nõuab avaliku sektori asutuse poolt või tema nimel osutatava internetipõhise teenuse kasutamiseks kvalifitseeritud sertifikaadil põhinevat täiustatud e-allkirja, tunnustab see liikmesriik kvalifitseeritud sertifikaadil põhinevaid täiustatud e-allkirju ja kvalifitseeritud e-allkirju, mis on antud vähemalt lõikes 5 osutatud formaadis või rakendusaktides määratletud meetodeid kasutades.

3. Liikmesriigid ei nõua avaliku sektori asutuse poolt osutatava internetipõhise teenuse piiriüleseks kasutamiseks e-allkirja, mille tagatistase on kõrgem kui kvalifitseeritud e-allkirjal.

4. Komisjon võib rakendusaktidega kehtestada täiustatud e-allkirjade standardite viitenumbrid. Kui täiustatud e-allkiri vastab neile standarditele, loetakse see käesoleva artikli lõigetes 1 ja 2 ning artiklis 26 täiustatud e-allkirjadele sätestatud nõuetele vastavaks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

5. Komisjon võtab kehtivaid tavasid, standardeid ja liidu õigusakte arvestades hiljemalt 18. septembriks 2015 vastu rakendusaktid, milles määratakse kindlaks täiustatud e-allkirjade standardformaadid või alternatiivsete formaatide kasutamise korral standardmeetodid. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 28

E-allkirjade kvalifitseeritud sertifikaadid

1. E-allkirjade kvalifitseeritud sertifikaadid peavad vastama I lisas sätestatud nõuetele.

2. E-allkirjade kvalifitseeritud sertifikaatide suhtes ei kohaldata ühtegi kohustuslikku nõuet, mis ületab I lisas sätestatud nõudeid.

3. E-allkirja kvalifitseeritud sertifikaadid võivad hõlmata mittekohustuslikke täiendavaid eritunnuseid. Need tunnused ei mõjuta kvalifitseeritud e-allkirjade koosvõimet ega tunnustamist.

4. Kui e-allkirjade kvalifitseeritud sertifikaat tühistatakse pärast esialgset aktiveerimist, kaotab see alates tühistamise hetkest kehtivuse ega saa oma staatust mingil juhul tagasi.

5. Liikmesriigid võivad järgmistel tingimustel kehtestada siseriiklikud eeskirjad e-allkirja kvalifitseeritud sertifikaatide ajutiseks peatamiseks:

a) kui e-allkirja kvalifitseeritud sertifikaat on ajutiselt peatatud, on kõnealune sertifikaat peatamise ajavahemikul kehtetu;

b) peatamise ajavahemik on sertifikaatide andmebaasis selgesti märgitud ja sertifikaatide staatuse kohta teavet andva teenuse kaudu saab peatamise ajavahemikul teavet peatamisstaatuse kohta.

6. Komisjon võib rakendusaktidega kehtestada e-allkirja kvalifitseeritud sertifikaatide standardite viitenumbrid. Kui e-allkirja kvalifitseeritud sertifikaat vastab kõnealustele standarditele, loetakse see I lisas sätestatud nõuetele vastavaks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 29

Nõuded kvalifitseeritud e-allkirja andmise vahenditele

1. Kvalifitseeritud e-allkirja andmise vahendid peavad vastama II lisas sätestatud nõuetele.

2. Komisjon võib rakendusaktidega kehtestada kvalifitseeritud e-allkirja andmise vahendite standardite viitenumbrid. Kui kvalifitseeritud e-allkirja andmise vahend vastab kõnealustele standarditele, loetakse see II lisas sätestatud nõuetele vastavaks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 30

Kvalifitseeritud e-allkirja andmise vahendite sertifitseerimine

1. Kvalifitseeritud e-allkirja andmise vahendite vastavust II lisas sätestatud nõuetele sertifitseerivad liikmesriikide määratud asjakohased avalik-õiguslikud või eraõiguslikud asutused.

2. Liikmesriigid teatavad komisjonile lõikes 1 osutatud avalik-õiguslike või eraõiguslike asutuste nimed ja aadressid. Komisjon teeb selle teabe liikmesriikidele kättesaadavaks.

3. Lõikes 1 osutatud sertifitseerimine põhineb ühel järgmistest võimalustest:

a) turvalisuse hindamise protsess, mis on tehtud kooskõlas ühega standarditest selliste infotehnoloogiatoodete turvalisuse hindamiseks, mis on kantud kooskõlas teise lõiguga koostatud nimekirja, või

b) punktis a osutatust erinev protsess, tingimusel et selles protsessis kasutatakse samaväärseid turvatasemeid ning et lõikes 1 osutatud avalik-õiguslik või eraõiguslik asutus teatab sellest protsessist komisjonile. Seda protsessi võib kasutada üksnes punktis a osutatud standardite puudumisel või juhul kui käimas on punktis a osutatud turvalisuse hindamise protsess.

Komisjon koostab rakendusaktidega punktis a osutatud infotehnoloogiatoodete turvalisuse hindamise standardite nimekirja. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

4. Komisjonile on õigus võtta kooskõlas artikliga 47 vastu delegeeritud õigusakte, et kehtestada konkreetsed kriteeriumid, millele käesoleva artikli lõikes 1 osutatud määratud asutused peavad vastama.

Artikkel 31

Sertifitseeritud kvalifitseeritud e-allkirja andmise vahendite nimekirja avaldamine

1. Liikmesriigid edastavad komisjonile põhjendamatu viivituseta ja mitte hiljem kui üks kuu pärast sertifitseerimise lõpuleviimist teabe selliste kvalifitseeritud e-allkirja andmise vahendite kohta, mille on sertifitseerinud artikli 30 lõikes 1 osutatud asutused. Samuti edastavad nad komisjonile põhjendamatu viivituseta ja mitte hiljem kui üks kuu pärast sertifitseerimise tühistamist teabe selliste kvalifitseeritud e-allkirja andmise vahendite kohta, mis ei ole enam sertifitseeritud.

2. Saadud teabe põhjal koostab komisjon sertifitseeritud kvalifitseeritud e-allkirja andmise vahendite nimekirja, haldab seda ja avaldab selle.

3. Komisjon võib rakendusaktidega kindlaks määrata lõike 1 kohaldamisega seotud formaadid ja menetlused. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 32

Nõuded kvalifitseeritud e-allkirjade valideerimisele

1. Kvalifitseeritud e-allkirja valideerimise protsess kinnitab kvalifitseeritud e-allkirja kehtivust, kui on täidetud järgmised tingimused:

a) allkirja kinnitav sertifikaat oli allkirja andmise ajal I lisa sätetele vastav kvalifitseeritud e-allkirja sertifikaat;

b) kvalifitseeritud sertifikaadi väljastas kvalifitseeritud usaldusteenuse osutaja ja sertifikaat oli allkirja andmise ajal kehtiv;

c) allkirja valideerimise andmed vastavad tuginevatele isikutele esitatud andmetele;

d) sertifikaadil olevat allkirja andjat tähistavad kordumatud andmed on nõuetekohaselt esitatud tuginevatele isikutele;

e) kui allkirja andmisel kasutati varjunime, on varjunime kasutus tuginevale isikule selgesti näidatud;

f) e-allkiri on antud kvalifitseeritud e-allkirja andmise vahendiga;

g) allkirjastatud andmete terviklust ei ole rikutud;

h) artiklis 26 sätestatud nõuded olid allkirja andmise ajal täidetud.

2. Kvalifitseeritud e-allkirja valideerimiseks kasutatav süsteem annab tuginevale isikule valideerimisprotsessi korrektse tulemuse ja võimaldab tugineval isikul tuvastada turvalisusega seotud probleeme.

3. Komisjon võib rakendusaktidega kehtestada kvalifitseeritud e-allkirjade valideerimise standardite viitenumbrid. Kui kvalifitseeritud e-allkirjade valideerimine vastab kõnealustele standarditele, loetakse see lõikes 1 sätestatud nõuetele vastavaks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 33

Kvalifitseeritud e-allkirjade kvalifitseeritud valideerimisteenus

1. Kvalifitseeritud e-allkirjade kvalifitseeritud valideerimisteenust võib osutada üksnes kvalifitseeritud usaldusteenuse osutaja, kes:

a) osutab valideerimisteenust kooskõlas artikli 32 lõikega 1 ja

b) võimaldab tuginevatel isikutel saada valideerimisprotsessi tulemuse automaatsel viisil, mis on usaldusväärne, tõhus ja millel on kvalifitseeritud valideerimisteenuse osutaja täiustatud e-allkiri või täiustatud e-tempel.

2. Komisjon võib rakendusaktidega kehtestada lõikes 1 osutatud kvalifitseeritud valideerimisteenuse standardite viitenumbrid. Kui kvalifitseeritud e-allkirjade valideerimisteenus vastab kõnealustele standarditele, loetakse see lõikes 1 sätestatud nõuetele vastavaks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 34

Kvalifitseeritud e-allkirjade kvalifitseeritud säilitamisteenus

1. Kvalifitseeritud e-allkirjade kvalifitseeritud säilitamise teenust võib osutada üksnes kvalifitseeritud usaldusteenuse osutaja, kes kasutab menetlusi ja tehnoloogiat, millega on võimalik tagada kvalifitseeritud e-allkirjade usaldusväärsus ka pärast nende tehnoloogilise kehtivusaja lõppemist.

2. Komisjon võib rakendusaktidega kehtestada kvalifitseeritud e-allkirjade kvalifitseeritud säilitamise teenuse standardite viitenumbrid. Kui kvalifitseeritud e-allkirjade kvalifitseeritud säilitamise teenuse suhtes kohaldatav kord vastab kõnealustele standarditele, loetakse see lõikes 1 sätestatud nõuetele vastavaks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

5. JAGU

E-tempel

Artikkel 35

E-templi õiguslik toime

1. E-templit ei käsitata õigusliku toimeta ega kohtumenetlustes kõlbmatu tõendina ainuüksi seetõttu, et see on elektroonilises vormis või ei vasta kvalifitseeritud e-templitele esitatavatele nõuetele.

2. Kvalifitseeritud e-templi puhul eeldatakse sellega seotud andmete terviklust ja nende andmete päritolu õigsust.

3. Ühes liikmesriigis väljastatud kvalifitseeritud sertifikaadil põhinevat kvalifitseeritud e-templit tunnustatakse kvalifitseeritud e-templina ka kõikides teistes liikmesriikides.

Artikkel 36

Nõuded täiustatud e-templile

Täiustatud e-tempel vastab järgmistele nõuetele:

a) see on seotud ainuüksi templi andjaga;

b) selle abil on võimalik templi andjat tuvastada;

c) see antakse e-templi loomiseks vajalike andmete abil, mida templi andja saab kõrge salastatuse taseme juures kasutada e-templi loomiseks, ning

d) see on seotud seda puudutavate andmetega sellisel viisil, et kõik hilisemad andmete muudatused on tuvastatavad.

Artikkel 37

E-templid avalikus teenistuses

1. Kui liikmesriik nõuab avaliku sektori asutuse poolt või tema nimel osutatava internetipõhise teenuse kasutamiseks täiustatud e-templit, tunnustab see liikmesriik täiustatud e-templeid, e-templi kvalifitseeritud sertifikaadil põhinevaid täiustatud e-templeid ja kvalifitseeritud e-templeid, mis on loodud vähemalt lõikes 5 osutatud formaadis või rakendusaktides määratletud meetodeid kasutades.

2. Kui liikmesriik nõuab avaliku sektori asutuse poolt või tema nimel osutatava internetipõhise teenuse kasutamiseks kvalifitseeritud sertifikaadil põhinevat täiustatud e-templit, tunnustab see liikmesriik kvalifitseeritud sertifikaadil põhinevaid täiustatud e-templeid ja kvalifitseeritud e-templeid, mis on loodud vähemalt lõikes 5 osutatud formaadis või rakendusaktides määratletud meetodeid kasutades.

3. Liikmesriigid ei nõua avaliku sektori asutuse poolt osutatava internetipõhise teenuse piiriüleseks kasutamiseks e-templit, mille turvatase on kõrgem kui kvalifitseeritud e-templil.

4. Komisjon võib rakendusaktidega kehtestada täiustatud e-templite standardite viitenumbrid. Kui täiustatud e-tempel vastab neile standarditele, loetakse see käesoleva artikli lõigetes 1 ja 2 ning artiklis 36 täiustatud e-templitele sätestatud nõuetele vastavaks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

5. Komisjon võtab kehtivaid tavasid, standardeid ja liidu õigusakte arvestades hiljemalt 18. septembriks 2015 vastu rakendusaktid, milles määratakse kindlaks täiustatud e-templite standardformaadid või alternatiivsete formaatide kasutamise korral standardmeetodid. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 38

E-templi kvalifitseeritud sertifikaadid

1. E-templi kvalifitseeritud sertifikaadid peavad vastama III lisas sätestatud nõuetele.

2. E-templi kvalifitseeritud sertifikaatide suhtes ei kohaldata ühtegi kohustuslikku nõuet, mis ületab III lisas sätestatud nõudeid.

3. E-templi kvalifitseeritud sertifikaadid võivad hõlmata mittekohustuslikke täiendavaid eritunnuseid. Need tunnused ei mõjuta kvalifitseeritud e-templite koosvõimet ega tunnustamist.

4. Kui e-templi kvalifitseeritud sertifikaat tühistatakse pärast esialgset aktiveerimist, kaotab see alates tühistamise hetkest kehtivuse ega saa oma staatust mingil juhul tagasi.

5. Liikmesriigid võivad järgmistel tingimustel kehtestada siseriiklikud eeskirjad e-templi kvalifitseeritud sertifikaatide ajutiseks peatamiseks:

a) kui e-templi kvalifitseeritud sertifikaat on ajutiselt peatatud, on kõnealune sertifikaat peatamise ajavahemikul kehtetu;

b) peatamise ajavahemik on sertifikaatide andmebaasis selgesti märgitud ja sertifikaatide staatuse kohta teavet andva teenuse kaudu saab peatamise ajavahemikul teavet sertifikaatide staatuse kohta.

6. Komisjon võib rakendusaktidega kehtestada e-templi kvalifitseeritud sertifikaatide standardite viitenumbrid. Kui e-templi kvalifitseeritud sertifikaat vastab kõnealustele standarditele, loetakse see III lisas sätestatud nõuetele vastavaks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 39

Kvalifitseeritud e-templi loomise vahendid

1. Kvalifitseeritud e-templi loomise vahendeid käsitlevate nõuete suhtes kohaldatakse *mutatis mutandis* artiklit 29.

2. Kvalifitseeritud e-templi loomise vahendite sertifitseerimise suhtes kohaldatakse *mutatis mutandis* artiklit 30.

3. Sertifitseeritud kvalifitseeritud e-templi loomise vahendite nimekirja avaldamise suhtes kohaldatakse *mutatis mutandis* artiklit 31.

Artikkel 40

Kvalifitseeritud e-templite valideerimine ja säilitamine

Kvalifitseeritud e-templite valideerimise ja säilitamise suhtes kohaldatakse *mutatis mutandis* artikleid 32, 33 ja 34.

6. JAGU

E-ajatemplid

Artikkel 41

E-ajatempli õiguslik toime

1. E-ajatemplit ei tunnistata õiguslikult kehtetuks ega kohtumenetlustes tõenduskõlbmatuks ainuüksi seetõttu, et see on elektroonilisel kujul või ei vasta kvalifitseeritud e-ajatemplitele esitatavatele nõuetele.

2. Kvalifitseeritud e-ajatempli suhtes kehtib sellega osutatava kuupäeva ja ajahetke täpsuse ja kõnealuse kuupäeva ja ajahetkega seotud andmete tervikluse eeldus.

3. Ühes liikmesriigis väljastatud kvalifitseeritud e-ajatemplit tunnustatakse kvalifitseeritud e-ajatemplina kõikides liikmesriikides.

Artikkel 42

Nõuded kvalifitseeritud e-ajatemplitele

1. Kvalifitseeritud e-ajatempel vastab järgmistele nõuetele:

a) see seob kuupäeva ja ajahetke andmetega sellisel viisil, mis mõistlikkuse piires välistab andmete tuvastamatu muutmise võimaluse;

b) see põhineb täpsel ajaallikal, mis on seotud koordineeritud maailmaajaga, ning

c) see on allkirjastatud kvalifitseeritud usaldusteenuse osutaja täiustatud e-allkirjaga või kinnitatud kvalifitseeritud usaldusteenuse osutaja täiustatud e-templiga või mõne muu samaväärse meetodi abil.

2. Komisjon võib rakendusaktidega kehtestada kuupäeva ja ajahetke andmetega sidumise ja täpsete ajaallikate standardite viitenumbrid. Kui kuupäeva ja ajahetke andmetega sidumine ja täpne ajaallikas vastavad kõnealustele standarditele, loetakse need lõikes 1 sätestatud nõuetele vastavaks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

7. JAGU

Registreeritud e-andmevahetusteenused

Artikkel 43

Registreeritud andmevahetusteenuse õiguslik toime

1. Registreeritud andmevahetusteenust kasutades saadetud ja kättesaadud andmeid ei tunnistata õiguslikult kehtetuks ega kohtumenetlustes tõenduskõlbmatuks ainuüksi seetõttu, et teenus on elektrooniline või ei vasta kvalifitseeritud registreeritud e-andmevahetusteenusele esitatavatele nõuetele.

2. Kvalifitseeritud registreeritud e-andmevahetusteenust kasutades saadetud ja kättesaadud andmete suhtes kehtib kvalifitseeritud registreeritud e-andmevahetusteenuse osutamisel märgitud andmete tervikluse, nende andmete identitud saatja poolse saatmise ja identitud adressaadi poolse kättesaamise ja nende andmete saatmise ja kättesaamise kuupäeva ja ajahetke täpsuse eeldus.

Artikkel 44

Nõuded kvalifitseeritud registreeritud e-andmevahetusteenustele

1. Kvalifitseeritud registreeritud e-andmevahetusteenused peavad vastama järgmistele nõuetele:

a) neid pakub üks või mitu kvalifitseeritud usaldusteenuse osutajat;

b) need tagavad saatja väga usaldusväärse identimise;

c) need tagavad adressaadi identimise enne andmete kättetoimetamist;

d) andmete saatmine ja kättesaamine on kaitstud kvalifitseeritud usaldusteenuse osutaja pakutava täiustatud e-allkirja või täiustatud e-tempiga viisil, mis välistab andmete tuvastamatu muutmise võimaluse;

e) mis tahes muudatusi andmete saatmiseks või kättesaamiseks vajalikes andmetes näidatakse andmete saatjale ja adressaadile selgesti;

f) andmete saatmise, kättesaamise ja mis tahes muudatuste tegemise kuupäev ja ajahetk näidatakse kvalifitseeritud e-ajatempliga.

Kui andmeid saadetakse kahe või enama kvalifitseeritud usaldusteenuse osutaja vahel, kohaldatakse punktides a–f osutatud nõudeid kõikide kvalifitseeritud usaldusteenuse osutajate suhtes.

2. Komisjon võib rakendusaktidega kehtestada andmete saatmise ja kättesaamise protsesse käsitlevate standardite viitenumbrid. Kui andmete saatmise ja kättesaamise protsess vastab kõnealustele standarditele, loetakse see lõikes 1 sätestatud nõuetele vastavaks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

8. JAGU

Veebisaidi autentimine

Artikkel 45

Nõuded veebisaidi autentimise kvalifitseeritud sertifikaatidele

1. Veebisaidi autentimise kvalifitseeritud sertifikaadid peavad vastama IV lisas sätestatud nõuetele.

2. Komisjon võib rakendusaktidega kehtestada veebisaidi autentimise kvalifitseeritud sertifikaatide standardite viitenumbrid. Kui veebisaidi autentimise kvalifitseeritud sertifikaat vastab kõnealustele standarditele, loetakse see IV lisas sätestatud nõuetele vastavaks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

IV PEATÜKK

E-DOKUMENDID

Artikkel 46

E-dokumentide õiguslik toime

E-dokumenti ei tunnistata õiguslikult kehtetuks ega kohtumenetlustes tõenduskõlbmatuks ainuüksi seetõttu, et see on elektroonilisel kujul.

V PEATÜKK

DELEGEERITUD ÕIGUSAKTID JA RAKENDUSAKTID

Artikkel 47

Delegeeritud volituste rakendamine

1. Komisjonile antakse õigus võtta vastu delegeeritud õigusakte käesolevas artiklis sätestatud tingimustel.

2. Artikli 30 lõikes 4 osutatud õigus võtta vastu delegeeritud õigusakte antakse komisjonile määramata ajaks alates 17. septembrist 2014.

3. Euroopa Parlament ja nõukogu võivad artikli 30 lõikes 4 osutatud volituste delegeerimise igal ajal tagasi võtta. Tagasivõtmise otsusega lõpetatakse otsuses nimetatud volituste delegeerimine. Otsus jõustub järgmisel päeval pärast selle avaldamist *Euroopa Liidu Teatajas* või otsuses nimetatud hilisemal kuupäeval. See ei mõjuta juba jõustunud delegeeritud õigusaktide kehtivust.

4. Niipea kui komisjon on delegeeritud õigusakti vastu võtnud, teeb ta selle samal ajal teatavaks Euroopa Parlamendile ja nõukogule.

5. Artikli 30 lõike 4 alusel vastu võetud delegeeritud õigusakt jõustub üksnes juhul, kui Euroopa Parlament ega nõukogu ei ole kahe kuu jooksul pärast õigusakti teatavakstegemist Euroopa Parlamendile ja nõukogule esitanud selle suhtes vastuväidet või kui Euroopa Parlament ja nõukogu on enne selle tähtaja möödumist komisjonile teatanud, et nad ei esita vastuväidet. Euroopa Parlamendi või nõukogu algatusel pikendatakse seda tähtaega kahe kuu võrra.

Artikkel 48

Komiteemenetlus

1. Komisjoni abistab komitee. Nimetatud komitee on komitee määruse (EL) nr 182/2011 tähenduses.

2. Käesolevale lõikele viitamisel kohaldatakse määruse (EL) nr 182/2011 artiklit 5.

VI PEATÜKK

LÕPPSÄTTED

Artikkel 49

Läbivaatamine

Komisjon vaatab läbi käesoleva määruse kohaldamise ja annab sellest Euroopa Parlamendile ja nõukogule aru hiljemalt 1. juuliks 2020. Komisjon hindab eelkõige seda, kas on asjakohane muuta käesoleva määruse kohaldamisala või selle erisätteid, sealhulgas artiklit 6, artikli 7 punkti f ja artikleid 34, 43, 44 ja 45, võttes arvesse käesoleva määruse kohaldamisel saadud kogemusi ning tehnoloogia, turu ja õiguse arengut.

Asjakohasel juhul lisatakse esimeses lõigus osutatud aruandele seadusandlikud ettepanekud.

Lisaks esitab komisjon Euroopa Parlamendile ja nõukogule iga nelja aasta järel pärast esimeses lõigus osutatud aruande esitamist aruande selle kohta, kuidas on edenenud käesoleva määruse eesmärkide saavutamine.

Artikkel 50

Kehtetuks tunnistamine

1. Direktiiv 1999/93/EÜ tunnistatakse kehtetuks alates 1. juulist 2016.

2. Viiteid kehtetukstunnistatud direktiivile käsitatakse viidetena käesolevale määrusele.

Artikkel 51

Üleminekumeetmed

1. Selliseid turvalisi allkirja andmise vahendeid, mille vastavus on direktiivi 1999/93/EÜ artikli 3 lõike 4 kohaselt kindlaks määratud, käsitatakse käesoleva määruse kohaselt kvalifitseeritud e-allkirja andmise vahenditena.

2. Direktiivi 1999/93/EÜ alusel füüsilistele isikutele väljastatud kvalifitseeritud sertifikaate käsitatakse käesoleva määruse kohaselt e-allkirja kvalifitseeritud sertifikaatidena kuni nende kehtivuse lõpuni.

3. Direktiivi 1999/93/EÜ alusel kvalifitseeritud sertifikaate väljastav sertifitseerimisteenuste osutaja esitab järelevalveasutusele võimalikult kiiresti, kuid mitte hiljem kui 1. juulil 2017 vastavushindamisaruande. Kuni sellise vastavushindamisaruande esitamiseni ja selle hindamise lõpuleviimiseni järelevalveasutuse poolt käsitatakse asjaomast sertifitseerimisteenuse osutajat käesoleva määruse kohase kvalifitseeritud usaldusteenuse osutajana.

4. Kui direktiivi 1999/93/EÜ alusel kvalifitseeritud sertifikaate väljastav sertifitseerimisteenuste osutaja ei esita järelevalveasutusele lõikes 3 osutatud tähtaja jooksul vastavushindamisaruannet, ei käsitata seda sertifitseerimisteenuste osutajat alates 2. juulist 2017 käesoleva määruse kohase kvalifitseeritud usaldusteenuse osutajana.

Artikkel 52

Jõustumine

1. Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas.*

2. Käesolevat määrust kohaldatakse alates 1. juulist 2016, välja arvatud järgmised sätted:

a) artikli 8 lõiget 3, artikli 9 lõiget 5, artikli 12 lõikeid 2–9, artikli 17 lõiget 8, artikli 19 lõiget 4, artikli 20 lõiget 4, artikli 21 lõiget 4, artikli 22 lõiget 5, artikli 23 lõiget 3, artikli 24 lõiget 5, artikli 27 lõikeid 4 ja 5, artikli 28 lõiget 6, artikli 29 lõiget 2, artikli 30 lõikeid 3 ja 4, artikli 31 lõiget 3, artikli 32 lõiget 3, artikli 33 lõiget 2, artikli 34 lõiget 2, artikli 37 lõikeid 4 ja 5, artikli 38 lõiget 6, artikli 42 lõiget 2, artikli 44 lõiget 2, artikli 45 lõiget 2 ning artikleid 47 ja 48 kohaldatakse alates 17. septembrist 2014;

b) artiklit 7, artikli 8 lõikeid 1 ja 2, artikleid 9, 10 ja 11 ning artikli 12 lõiget 1 kohaldatakse alates artikli 8 lõikes 3 ja artikli 12 lõikes 8 osutatud rakendusaktide kohaldamise alguskuupäevast;

c) artiklit 6 kohaldatakse kolm aastat alates artikli 8 lõikes 3 ja artikli 12 lõikes 8 osutatud rakendusaktide kohaldamise alguskuupäevast.

3. Kui teadaantud e-identimise süsteem on nimekirjas, mille komisjon avaldab artikli 9 kohaselt enne käesoleva artikli lõike 2 punktis c osutatud kuupäeva, tunnustatakse selle süsteemi kohast e-identimise vahendit vastavalt artiklile 6 hiljemalt 12 kuud pärast vastava süsteemi avaldamist, kuid mitte enne käesoleva artikli lõike 2 punktis c osutatud kuupäeva.

4. Ilma et see piiraks käesoleva artikli lõike 2 punkti c kohaldamist, võib liikmesriik otsustada, et muu liikmesriigi poolt artikli 9 lõike 1 kohaselt teada antud e-identimise süsteemi kohaseid e-identimise vahendeid tunnustatakse esimesena nimetatud liikmesriigis alates artikli 8 lõikes 3 ja artikli 12 lõikes 8 osutatud rakendusaktide kohaldamise kuupäevast. Asjaomased liikmesriigid teavitavad sellest komisjoni. Komisjon avalikustab nimetatud teabe.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 23. juuli 2014

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*
M. SCHULZ	S. GOZI

I LISA

NÕUDED E-ALLKIRJA KVALIFITSEERITUD SERTIFIKAATIDELE

E-allkirja kvalifitseeritud sertifikaadid peavad sisaldama järgmist:

a) vähemalt automaatseks töötlemiseks sobivas formaadis märge selle kohta, et sertifikaat on väljastatud e-allkirja kvalifitseeritud sertifikaadina;

b) kvalifitseeritud sertifikaate väljastava kvalifitseeritud usaldusteenuse osutajat üheselt mõistetavalt tähistavad andmed, mis sisaldavad vähemalt selle liikmesriigi nime, kus kõnealune teenuseosutaja asub, ning

— kui tegemist on juriidilise isikuga: nimi ja kui see on asjakohane, siis registrinumber, nagu see on esitatud ametlikes dokumentides,

— kui tegemist on füüsilise isikuga: isiku nimi;

c) vähemalt allkirja andja nimi või varjunimi; kui kasutatakse varjunime, on varjunime kasutus selgesti näidatud;

d) e-allkirja valideerimisandmed, mis vastavad e-allkirja andmiseks vajalikele andmetele;

e) üksikasjalikud andmed sertifikaadi kehtivusaja alguse ja lõpu kohta;

f) kvalifitseeritud usaldusteenuse osutajale omistatud ainukordne sertifikaadi tunnuskood;

g) väljastava kvalifitseeritud usaldusteenuse osutaja täiustatud e-allkiri või täiustatud e-tempel;

h) koht, kus punktis g osutatud täiustatud e-allkirja või täiustatud e-templit kinnitav sertifikaat on tasuta kättesaadav;

i) nende teenuste koht, mille abil on võimalik uurida kvalifitseeritud sertifikaadi kehtivust;

j) kui e-allkirja valideerimisandmetega seotud e-allkirja andmiseks vajalikud andmed asuvad kvalifitseeritud e-allkirja andmise vahendis, siis vähemalt automaatseks töötlemiseks sobivas formaadis asjakohane viide kõnealusele kohale.

II LISA

NÕUDED KVALIFITSEERITUD E-ALLKIRJA ANDMISE VAHENDITELE

1. Kvalifitseeritud e-allkirja andmise vahendid tagavad asjakohaste tehniliste ja menetluslike vahendite abil vähemalt selle, et:

   a) e-allkirja andmiseks kasutatavate e-allkirja andmiseks vajalike andmete konfidentsiaalsus on piisavalt tagatud;

   b) e-allkirja andmiseks kasutatavad e-allkirja andmiseks vajalikud andmed võivad reaalselt esineda ainult ühe korra;

   c) on piisavalt kindel, et e-allkirja andmiseks kasutatavaid e-allkirja andmiseks vajalikke andmeid ei saa tuletada ja et e-allkiri on piisavalt kaitstud praegu kättesaadava tehnoloogia abil võltsimise vastu;

   d) õiguspärane allkirja andja saab e-allkirja andmiseks kasutatavaid e-allkirja andmiseks vajalikke andmeid piisavalt kaitsta, et teised isikud ei saaks neid kasutada.

2. Kvalifitseeritud e-allkirja andmise vahendid ei tohi muuta allkirjastatavaid andmeid ega takistada selliste andmete esitamist allkirja andjale enne allkirja andmist.

3. E-allkirja andmiseks vajalikke andmeid võib allkirja andja nimel luua või hallata üksnes kvalifitseeritud usaldusteenuse osutaja.

4. Ilma et see piiraks punkti 1 alapunkti d kohaldamist, võib kvalifitseeritud usaldusteenuse osutaja, kes haldab e-allkirja andmiseks vajalikke andmeid allkirja andja nimel, dubleerida e-allkirja andmiseks vajalikud andmed üksnes varukoopiate omamiseks, eeldusel et on täidetud järgmised tingimused:

   a) dubleeritud andmekogumi turvatase peab olema sama mis algsel andmekogumil;

   b) dubleeritud andmekogumite arv ei ületa teenuse järjepidevuse tagamiseks vajalikku miinimumi.

III LISA

NÕUDED E-TEMPLITE KVALIFITSEERITUD SERTIFIKAATIDELE

E-templite kvalifitseeritud sertifikaadid peavad sisaldama järgmist:

a) vähemalt automaatseks töötlemiseks sobivas formaadis märge selle kohta, et sertifikaat on väljastatud e-templi kvalifitseeritud sertifikaadina;

b) kvalifitseeritud sertifikaate väljastava kvalifitseeritud usaldusteenuse osutajat üheselt mõistetavalt tähistavad andmed, mis sisaldavad vähemalt selle liikmesriigi nime, kus teenuseosutaja asub, ning

— kui tegemist on juriidilise isikuga: nimi ja kui see on asjakohane, siis registrinumber, nagu see on esitatud ametlikes dokumentides,

— kui tegemist on füüsilise isikuga: isiku nimi;

c) vähemalt e-templi andja nimi ja kui see on asjakohane, siis registrinumber, nagu see on esitatud ametlikes dokumentides;

d) e-templi valideerimisandmed, mis vastavad e-templi loomiseks vajalikele andmetele;

e) üksikasjalikud andmed sertifikaadi kehtivusaja alguse ja lõpu kohta;

f) kvalifitseeritud usaldusteenuse osutajale omistatud ainukordne sertifikaadi tunnuskood;

g) väljastava kvalifitseeritud usaldusteenuse osutaja täiustatud e-allkiri või täiustatud e-tempel;

h) koht, kus punktis g osutatud täiustatud e-allkirja või täiustatud e-templit kinnitav sertifikaat on tasuta kättesaadav;

i) nende teenuste koht, mille abil on võimalik uurida kvalifitseeritud sertifikaadi kehtivust;

j) kui e-templi valideerimisandmetega seotud e-templi loomiseks vajalikud andmed asuvad kvalifitseeritud e-templi loomise vahendis, siis vähemalt automaatseks töötlemiseks sobivas formaadis asjakohane viide kõnealusele kohale.

IV LISA

NÕUDED VEEBISAIDI AUTENTIMISE KVALIFITSEERITUD SERTIFIKAATIDELE

Kvalifitseeritud sertifikaadid veebisaidi autentimiseks peavad sisaldama järgmist:

a) vähemalt automaatseks töötlemiseks sobivas formaadis märge selle kohta, et sertifikaat on väljastatud veebisaidi autentimise kvalifitseeritud sertifikaadina;

b) kvalifitseeritud sertifikaate väljastava kvalifitseeritud usaldusteenuse osutajat üheselt mõistetavalt tähistavad andmed, mis sisaldavad vähemalt selle liikmesriigi nime, kus teenuseosutaja asub, ning

— kui tegemist on juriidilise isikuga: nimi ja kui see on asjakohane, siis registrinumber, nagu see on esitatud ametlikes dokumentides,

— kui tegemist on füüsilise isikuga: isiku nimi;

c) kui tegemist on füüsilise isikuga: vähemalt selle isiku nimi või varjunimi, kellele sertifikaat on väljastatud. Kui kasutatakse varjunime, on varjunime kasutus selgesti näidatud;

kui tegemist on juriidilise isikuga: vähemalt selle juriidilise isiku nimi, kellele sertifikaat on väljastatud, ja kui see on asjakohane, siis registrinumber, nagu see on esitatud ametlikes dokumentides;

d) selle füüsilise või juriidilise isiku aadressi elemendid, kellele sertifikaat on väljastatud, sealhulgas vähemalt linn ja riik; kui see on asjakohane, siis sellisel kujul, nagu need on esitatud ametlikes dokumentides;

e) selle domeeni nimi/nende domeenide nimed, mida haldab füüsiline või juriidiline isik, kellele sertifikaat on väljastatud;

f) üksikasjalikud andmed sertifikaadi kehtivusaja alguse ja lõpu kohta;

g) kvalifitseeritud usaldusteenuse osutajale omistatud ainukordne sertifikaadi tunnuskood;

h) väljastava kvalifitseeritud usaldusteenuse osutaja täiustatud e-allkiri või täiustatud e-tempel;

i) koht, kus punktis h osutatud täiustatud e-allkirja või täiustatud e-templit kinnitav sertifikaat on tasuta kättesaadav;

j) nende sertifikaadi kehtivusega seotud teenuste koht, mille abil on võimalik uurida kvalifitseeritud sertifikaadi kehtivust.