Euroopa Liidu
Nõukogu

Brüssel, 6. detsember 2022
(OR. en)

15706/22

Institutsioonidevaheline dokument: 2021/0136(COD)

TELECOM 519
COMPET 1006
MI 919
DATAPROTECT 352
JAI 1634
CODEC 1941

MENETLUSE TULEMUS

Saatja:	Nõukogu peasekretariaat
Kuupäev:	6. detsember 2022
Saaja:	Delegatsioonid
Eelmise dok nr:	14959/22 + ADD 1 + ADD 2
Komisjoni dok nr:	9471/21
Teema:	Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega muudetakse määrust (EL) nr 910/2014 seoses Euroopa digiidentiteedi raamistiku kehtestamisega - Üldine lähenemisviis (6. detsember 2022)

Delegatsioonidele edastatakse lisas eespool nimetatud ettepanekut käsitlev nõukogu üldine lähenemisviis, mille nõukogu kiitis heaks oma 6. detsembril 2022 toimunud 3917. istungil (transport, telekommunikatsioon ja energeetika).

Üldises lähenemisviisis määrataks kindlaks nõukogu esialgne seisukoht käesoleva ettepaneku suhtes ning see oleks aluseks ettevalmistustele, mida tehakse läbirääkimiste pidamiseks Euroopa Parlamendiga.

LISA

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

millega muudetakse määrust (EL) nr 910/2014 seoses Euroopa digiidentiteedi raamistiku kehtestamisega

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

ning arvestades järgmist:

(1) Komisjoni 19. veebruari 2020. aasta teatises „Euroopa digituleviku kujundamine“[2] teatatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 läbivaatamisest, et muuta selle toimimine tõhusamaks, laiendada selle positiivset mõju erasektorile ja edendada usaldusväärseid digiidentiteete kõigi eurooplaste jaoks.

[1] ELT C ..., ..., lk …
[2] COM(2020) 67 final.

(2) Euroopa Ülemkogu kutsus oma 1.– 2. oktoobri 2020. aasta järeldustes[3] komisjoni üles tegema ettepanekut töötada välja kogu ELi hõlmav turvalise avaliku elektroonilise identimise (e-ID) raamistik, sealhulgas koostalitlusvõimelised digitaalallkirjad, et anda inimestele kontroll oma internetiidentiteedi ja andmete üle ning võimaldada juurdepääsu avalikele, eraõiguslikele ja piiriülestele digiteenustele.

(3) Komisjoni 9. märtsi 2021. aasta teatises „Digikompass 2030: Euroopa tee digikümnendil“[4] esitatakse eesmärgiks liidu raamistik, mis peaks aastaks 2030 viima usaldusväärse ja kasutaja kontrolli all oleva identiteedi ulatusliku kasutuselevõtuni, mis võimaldaks igal kodanikul kontrollida oma toiminguid ja enda kohta internetis olevaid andmeid.

(4) Ühtsem lähenemisviis e-identimisele peaks vähendama riske ja kulusid, mille põhjus on praegune erinevate riiklike lahenduste kasutamisest tulenev killustatus, ning see tugevdab ühtset turgu, võimaldades kodanikel, muudel siseriiklikes õigusaktides määratletud elanikel ja ettevõtjatel kogu liidus internetis mugavalt ja ühetaoliselt oma isikut tõendada. Euroopa digiidentiteeditasku annab füüsilistele ja juriidilistele isikutele kogu liidus ühtlustatud e-identimise vahendi, mis võimaldab neil oma identiteediga seotud andmeid autentida ja jagada. Igaühel peaks olema turvaline juurdepääs avalikele ja erateenustele, mis põhinevad usaldusteenuste täiustatud ökosüsteemil ning kontrollitud isikut tõendavatel dokumentidel ja sellistel tõenditel teatud atribuutide kohta nagu ülikoolidiplom, mida tunnustatakse ja aktsepteeritakse kõikjal liidus. Euroopa digiidentiteedi raamistiku eesmärk on minna üksnes riiklikele digitaalse identiteedi lahendustele tuginemiselt üle Euroopa tasandil kehtivate atribuutide elektrooniliste tõendite esitamisele. Atribuutide elektroonilise tõendamise teenuse pakkujate suhtes tuleks kohaldada selgeid ja ühtseid norme ning haldusasutused peaksid saama tugineda teatavas vormingus elektroonilistele dokumentidele.

---

[3] https://www.consilium.europa.eu/et/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/.

[4] COM(2021) 118 final/2.

(4a) Mitu liikmesriiki on kasutusele võtnud ja kasutavad valdavalt selliseid e-identimise vahendeid, mida liidu teenuseosutajad tänapäeval aktsepteerivad. Lisaks on tehtud investeeringuid nii riiklikesse kui ka piiriülestesse kehtival eIDASe määrusel põhinevatesse lahendustesse, sealhulgas eIDAS-sõlmede koostalitlusvõime tehnilisse taristusse. Selleks et tagada Euroopa digiidentiteeditaskute vastastikune täiendavus ja kiire kasutuselevõtt teavitatud e-identimise vahendite praeguste kasutajate poolt ning minimeerida mõju olemasolevatele teenuseosutajatele, eeldatakse, et Euroopa digiidentiteeditaskud toetuvad olemasolevate e-identimise vahenditega saadud kogemustele ning kasutavad ära Euroopa ja liikmesriikide tasandil kasutusele võetud eIDASe taristut.

(5) Euroopa ettevõtjate konkurentsivõime toetamiseks peaks internetipõhiste teenuste osutajatel olema võimalik tugineda digiidentiteedi lahendustele, mida tunnustatakse kogu liidus, olenemata liikmesriigist, kus neid pakutakse, ning saada seega kasu ühtlustatud Euroopa lähenemisviisist usaldusele, turvalisusele ja koostalitlusvõimele. Nii kasutajatel kui ka teenuseosutajatel peaks olema kindlus, et atribuutide elektroonilisel tõendamisel on sama õigusjõud kogu liidus.

(6) Käesoleva määruse rakendamisel toimuva isikuandmete töötlemise suhtes kohaldatakse määrust (EL) 2016/679[5]. Seepärast tuleks käesolevas määruses sätestada konkreetsed kaitsemeetmed, et e-identimise vahendite ja atribuutide elektroonilise tõendamise teenuse pakkujad ei saaks kombineerida muudest teenustest pärinevaid isikuandmeid käesoleva määruse kohaldamisalasse kuuluvate teenustega seotud isikuandmetega. Euroopa digiidentiteeditaskute pakkumisega seotud isikuandmeid tuleks loogiliselt lahus hoida kõigist muudest andmetest, mida väljastaja säilitab. Käesolev määrus ei takista Euroopa digiidentiteeditaskute väljastajaid võtmast täiendavaid tehnilisi meetmeid, mis aitavad kaitsta isikuandmeid, nagu digiidentiteeditaskute pakkumisega seotud isikuandmete füüsiline eraldamine muudest andmetest, mida väljastaja säilitab.

---

[5] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

(7) On vaja kehtestada ühtlustatud tingimused liikmesriikide poolt pakutavate Euroopa digiidentiteeditaskute raamistiku loomiseks, mis peaks andma kõigile liidu kodanikele ja teistele siseriiklikes õigusaktides määratletud elanikele võimaluse jagada turvaliselt oma identiteediga seotud andmeid kasutajasõbralikul ja mugaval viisil kasutaja ainukontrolli all. Nende eesmärkide saavutamiseks tuleks välja töötada kõrgeima turvalisuse taseme, privaatsuse, kasutajamugavuse ja laia kasutatavuse poole püüdlev tehnoloogia. Liikmesriigid peaksid tagama kõigile oma kodanikele ja elanikele võrdse juurdepääsu e-identimisele.

(8) Selleks et tuginevad isikud saaksid tugineda Euroopa digiidentiteeditaskute kasutamisele ja kaitsta kasutajat tundlike andmete ebaseadusliku kasutamise eest, tuleks tuginevad isikud registreerida teavitamise protsessi osana. Tuginevate isikute suhtes kohaldatavad teavitamisnõuded peaksid enamikul juhtudel põhinema piiratud hulgal teabe esitamisel, mida on vaja tugineva isiku autentimiseks Euroopa digiidentiteeditasku jaoks. Need nõuded peaksid võimaldama ka automaatsete või lihtsate iseteavitamise menetluste kasutamist, sealhulgas seda, et liikmesriigid tuginevad olemasolevatele registritele ja kasutavad neid. Samal ajal võib tundlike andmete kategooriate suhtes kehtida riigi või liidu tasandil erikord, millega võidakse tuginevatele isikutele kehtestada rangemad registreerimis- ja loanõuded, et vältida sellistel juhtudel identiteediandmete ebaseaduslikku kasutamist. Muudel kasutusjuhtudel võidakse tuginevad isikud vabastada kohustusest teatada oma kavatsusest tugineda Euroopa digiidentiteeditaskule, näiteks kui konkreetsete atribuutide kontrollimise õigus ei nõua ega võimalda tugineva isiku autentimist elektrooniliste vahendite abil. Füüsiliste kohtumiste puhul saab kasutaja tavaliselt teha tugineva isiku kindlaks konteksti põhjal, näiteks autorenditöötaja või apteekriga suheldes. Teavitamisprotsess peaks toimuma valdkondlike liidu või liikmesriikide õigusaktide alusel, kuna see võimaldab arvesse võtta erinevaid kasutusjuhtumeid, mis võivad erineda registreerimisnõuete, tööreżiimi (võrgus toimuv / võrguväline) või Euroopa digiidentiteeditaskuga liidestamiseks sobivate seadmete autentimise nõude poolest. Euroopa digiidentiteeditasku tuginevate isikute poolt kasutamise kontrollimist ei tohiks nõuda Euroopa digiidentiteeditasku tasandil.

(9) Kõik Euroopa digiidentiteeditaskud peavad võimaldama kasutajatel end piiriüleselt elektrooniliselt identida ja autentida nii võrgus kui ka võrguväliselt, et pääseda juurde mitmesugustele avalikele ja erateenustele. Ilma et see piiraks liikmesriikide eelisõigusi oma kodanike ja elanike identimisel, võib digiidentiteeditasku täita ka haldusasutuste, rahvusvaheliste organisatsioonide ning liidu institutsioonide, organite ja asutuste institutsioonilisi vajadusi. Võrguväline kasutamine oleks oluline paljudes sektorites, sealhulgas tervishoiusektoris, kus teenuseid osutatakse sageli vahetult inimesega suheldes, ning digiretseptide puhul peaks autentsuse kontrollimiseks olema võimalik tugineda QR-koodidele või sarnasele tehnoloogiale. Tuginedes kõrgele usaldusväärsuse tasemele, peaksid Euroopa digiidentiteeditaskud saama käesoleva määruse kohaste turvanõuete täitmisel kasu võltsimiskindlate lahenduste, näiteks turvaelementide potentsiaalist. Euroopa digiidentiteeditaskud peaksid samuti võimaldama kasutajatel luua ja kasutada kogu ELis aktsepteeritavaid kvalifitseeritud e-allkirju ja e-templeid. Lihtsustamise eesmärgil ning inimeste ja ettevõtjate kulude vähendamiseks kogu ELis, sealhulgas võimaldades esindusõiguste ja e-volituste andmist, peaksid liikmesriigid väljastama ühistele standarditele tuginevaid Euroopa digiidentiteeditaskuid, et tagada sujuv koostalitlusvõime ja kõrge turvalisuse tase. Ainult liikmesriikide pädevad asutused saavad tagada usaldusväärsuse isikusamasuse tuvastamisel ja anda seega kindluse, et ennast teatud isikuna esitlev isik on tõepoolest isik, kes ta väidab end olevat. Seepärast peaksid Euroopa digiidentiteeditaskud põhinema kodanike, muude elanike või juriidiliste isikute õiguslikult määratletud identiteedil. Usaldust Euroopa digiidentiteeditaskute vastu suurendaks asjaolu, et neid väljastavad pooled peavad rakendama asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada kooskõlas määrusega (EL) 2016/679 turvalisuse tase, mis vastab füüsiliste isikute õigusi ja vabadusi ähvardavatele ohtudele. Euroopa digiidentiteeditaskute väljastamine, autentimiseks kasutamine ja tühistamine on füüsilistele isikutele tasuta. Digiidentiteeditasku kasutamisele tuginevate teenustega võivad kaasneda kulud, näiteks seoses atribuutide elektrooniliste tõendite väljastamisega digiidentiteeditaskule.

(9a) Kasulik on hõlbustada Euroopa digiidentiteeditaskute kasutuselevõttu ja kasutamist, integreerides need sujuvalt juba riiklikul, kohalikul või piirkondlikul tasandil kasutatavasse avaliku ja erasektori digiteenuste ökosüsteemi. Selle eesmärgi saavutamiseks võivad liikmesriigid näha ette õiguslikud ja korralduslikud meetmed, et suurendada paindlikkust Euroopa digiidentiteeditaskute väljastajate jaoks ja võimaldada Euroopa digiidentiteeditaskute lisafunktsioone lisaks käesolevas määruses sätestatule, sealhulgas suurendades koostalitlusvõimet olemasolevate riiklike e-identimise vahenditega. Sellega ei tohiks mingil juhul kahjustada käesolevas määruses sätestatud Euroopa digiidentiteeditaskute põhifunktsioonide täitmist ega edendada Euroopa digiidentiteeditaskute asemel olemasolevaid riiklikke lahendusi. Kuna need lisafunktsioonid ulatuvad käesolevast määrusest kaugemale, ei kohaldata nende suhtes käesolevas määruse sätteid, mis käsitlevad piiriülest tuginemist Euroopa digiidentiteeditaskutele.

(10) Andmekaitse, turvalisuse ja usaldusväärsuse kõrge taseme saavutamiseks tuleks käesoleva määrusega kehtestada ühtlustatud raamistik, milles kirjeldatakse üksikasjalikult Euroopa digiidentiteeditaskute suhtes kohaldatavaid ühiseid spetsifikatsioone ja nõudeid. Euroopa digiidentiteeditaskute vastavust neile nõuetele peaksid sertifitseerima liikmesriikide määratud akrediteeritud vastavushindamisasutused. Sertifitseerimine peaks tuginema eelkõige asjakohastele Euroopa küberturvalisuse sertifitseerimise kavadele või nende osadele, mis on kehtestatud vastavalt määrusele (EL) 2019/881,[6] niivõrd kui need hõlmavad Euroopa digiidentiteeditaskute suhtes kohaldatavaid küberturvalisuse nõudeid. Euroopa küberturvalisuse sertifitseerimise kavadele tuginemine peaks tagama ühtlustatud tasemel usalduse Euroopa digiidentiteeditaskute turvalisuse suhtes, olenemata sellest, kus need on liidus väljastatud. Euroopa digiidentiteeditaskute küberturvalisuse sertifitseerimine peaks tuginema riiklike küberturvalisuse sertifitseerimise asutuste rollile, et kontrollida ja jälgida nende jurisdiktsiooni alla kuuluvate vastavushindamisasutuste väljastatud sertifikaatide vastavust asjakohastele Euroopa küberturvalisuse kavadele. Samamoodi peaks sertifitseerimine vajaduse korral kasutama ära määruses (EL) 2019/881 sätestatud standardeid ja tehnilisi kirjeldusi. Selliseid kirjeldusi võib kasutada tipptaset esindavate dokumentidena, nagu on täpsustatud määruse (EL) 2019/881 kohastes asjakohastes küberturvalisuse sertifitseerimise kavades. Kui ükski määruse (EL) 2019/881 kohaselt loodud asjakohane Euroopa küberturvalisuse sertifitseerimise kava ei hõlma selliste asjakohaste teenuste või protsesside sertifitseerimist, mis aitavad kaasa digiidentiteeditasku turvalisusele, tuleks sellised asjakohased kavad kooskõlas määruse (EL) 2019/881 III jaotisega luua. Tuleks luua ühine ja ühtlustatud süsteem Euroopa digiidentiteeditaskute sertifitseerimiseks, et hinnata nende vastavust käesolevas määruses sätestatud ühtsetele spetsifikatsioonidele ja nõuetele, välja arvatud küberturvalisuse ja andmekaitsega seotud nõuetele, eelkõige funktsionaalseid ja toimimisega seotud aspekte hõlmavatele nõuetele. Seoses kõnealuse sertifitseerimisega tuleks usalduse ja läbipaistvuse kõrge taseme tagamiseks kehtestada mehhanismid ja menetlused, mille eesmärk on edendada vastastikust õppimist ja liikmesriikidevahelist koostööd sertifitseerimisasutuste ning nende väljastatavate sertifikaatide ja sertifitseerimisaruannete järelevalve ja läbivaatamise valdkonnas. Selline vastastikuse õppimise mehhanism ei tohiks piirata määruse (EL) 2016/679 ega määruse (EL) 2019/881 kohaldamist. Digiidentiteeditasku sertifitseerimine määruse (EL) 2016/679 alusel on vabatahtlik vahend, mida saab teiste hulgas kasutada selleks, et tõendada vastavust määruses (EL) 2016/679 sätestatud nõuetele, mida kohaldatakse Euroopa digiidentiteeditaskute ja nende Euroopa kodanikele pakkumise suhtes.

[6] Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 15).

(10a) Kodanike ja elanike Euroopa digiidentiteeditasku kasutajaks registreerimist tuleks hõlbustada, tuginedes kõrgel usaldusväärsuse tasemel väljastatud e-identimise vahenditele. Märkimisväärsel usaldusväärsuse tasemel välja antud e-identimise vahenditele tuleks tugineda ainult juhul, kui märkimisväärsel usaldusväärsuse tasemel väljastatud e-identimise vahendeid kasutavad ühtlustatud tehnilised kirjeldused ja tegevusspetsifikatsioonid koos muude täiendavate isikusamasuse kontrollimise vahenditega võimaldavad täita käesolevas määruses seoses kõrge usaldusväärsuse tasemega sätestatud nõudeid. Sellised täiendavad vahendid või meetmed peaksid olema usaldusväärsed ja kasutajate jaoks kergesti kasutatavad ning need võiksid tugineda võimalusele kasutada kaugregistreerimisprotseduure, kvalifitseeritud sertifikaate, mida toetavad kvalifitseeritud allkirjad, kvalifitseeritud elektroonilisi atribuutide tõendeid või nende kombinatsiooni. Selleks et tagada Euroopa digiidentiteeditaskute piisav kasutuselevõtt, tuleks rakendusaktides sätestada ühtlustatud tehnilised kirjeldused ja tegevusspetsifikatsioonid kasutajate registreerimiseks e-identimise vahendite abil, sealhulgas märkimisväärse usaldusväärsuse tasemel väljastatud vahendite abil.

(10b) Käesoleva määruse eesmärk on pakkuda kasutajale täielikult mobiilset, turvalist ja kasutajasõbralikku Euroopa digiidentiteeditaskut. Üleminekumeetmena kuni sertifitseeritud võltsimiskindlate lahenduste, näiteks kasutajate seadmetes sisalduvate turvaelementide kättesaadavuseni võivad Euroopa digiidentiteeditaskud krüptograafilise materjali ja muude tundlike andmete kaitsmisel tugineda sertifitseeritud välistele turvaelementidele või teatatud kõrgel usaldusväärsuse tasemel pakutavatele riiklikele lahendustele, et tõendada vastavust asjakohastele digiidentiteeditasku usaldusväärsuse taset käsitlevatele määruse nõuetele. Eespool nimetatud üleminekumeetme kasutamine peaks piirduma juhtudega, mille puhul on nõutav kõrge usaldusväärsuse tase, näiteks digiidentiteeditasku kasutajaks registreerimine ja kõrget usaldusväärsuse taset nõudvate teenuste kasutamiseks autentimine. Autentimisel märkimisväärset usaldusväärsuse taset nõudvate teenuste kasutamiseks ei peaks Euroopa digiidentiteeditaskud nõudma eespool nimetatud üleminekumeetme kasutamist. Kui kõnealune üleminekumeede tugineb sertifitseeritud välisele turvaelemendile, , ei tohiks käesolev määrus piirata nende väljastamise ja kasutamise siseriiklike tingimuste kohaldamist.

(11) Euroopa digiidentiteeditaskud peaksid tagama autentimiseks kasutatavate isikuandmete kõrgeima kaitse ja turvalisuse taseme, olenemata sellest, kas neid andmeid säilitatakse kohalikul tasandil või pilvepõhistes lahendustes, võttes arvesse erinevaid riskitasemeid. Biomeetriliste andmete töötlemine autentimistegurina tugeva kasutaja autentimise puhul on üks kõrge usaldusväärsusega identimismeetoditest, eriti kui seda kasutatakse koos muude autentimiselementidega. Kuna biomeetrilised andmed on iga isiku kordumatud omadused, on biomeetriliste andmete töötlemine lubatud üksnes määruse (EL) 2016/679 artikli 9 lõikes 2 sätestatud erandite alusel ning selleks on vaja asjakohaseid kaitsemeetmeid, mis vastavad ohule, mida selline töötlemine võib põhjustada füüsiliste isikute õigustele ja vabadustele.

(11a) Euroopa digiidentiteeditaskute toimimine peaks olema läbipaistev ja võimaldama isikuandmete kontrollitavat töötlemist. Selle saavutamiseks julgustatakse liikmesriike avalikustama Euroopa digiidentiteeditaskute isikuandmete ja juriidiliste isikute andmete töötlemisega seotud tarkvarakomponentide lähtekood. Sellise lähtekoodi avalikustamine võimaldab ühiskonnal, sealhulgas kasutajatel ja arendajatel, mõista selle toimimist. See võib suurendada ka kasutajate usaldust digiidentiteeditasku ökosüsteemi vastu ja aidata kaasa digiidentiteeditasku turvalisusele, võimaldades igaühel anda märku koodi nõrkustest ja vigadest. See innustab tarnijaid pakkuma ja hoidma töös toodet, mis on väga turvaline. Lisaks ja vajaduse korral julgustatakse liikmesriike samuti tegema lähtekoodi kättesaadavaks avatud lähtekoodi litsentsi alusel. Avatud lähtekoodi litsents võimaldab ühiskonnal, sealhulgas kasutajatel ja arendajatel lähtekoodi muuta ja taaskasutada.

(12) Tagamaks, et Euroopa digiidentiteedi raamistik on avatud innovatsioonile ja tehnoloogiaarendusele ning on tulevikukindel, tuleks liikmesriike üles kutsuda looma ühiselt testimiskeskkondi uuenduslike lahenduste katsetamiseks kontrollitud ja turvalises keskkonnas, eelkõige selleks, et parandada lahenduste funktsionaalsust, isikuandmete kaitset, turvalisust ja koostalitlusvõimet ning anda teavet tehniliste viidete ja õiguslike nõuete edaspidiseks ajakohastamiseks. See keskkond peaks soodustama Euroopa väikeste ja keskmise suurusega ettevõtjate, idufirmade ning üksikisikutest novaatorite ja teadlaste osalemist.

(13) Määrusega (EL) nr 2019/1157[7] suurendatakse isikutunnistuste turvalisust 2021. aasta augustiks täiustatud turvaelementidega. Liikmesriigid peaksid kaaluma võimalust teatada nendest e-identimise süsteemide raames, et laiendada e-identimise vahendite piiriülest kättesaadavust.

(14) E-identimise süsteemidest teavitamise korda tuleks lihtsustada ja kiirendada, et edendada juurdepääsu hõlpsasti kasutatavatele, usaldusväärsetele, turvalistele ja uuenduslikele autentimis- ja identimislahendustele ning vajaduse korral julgustada eraõiguslikke identimisteenuste osutajaid pakkuma e-identimise süsteeme liikmesriikide ametiasutustele teatamiseks määruse 910/2014 kohaste riiklike e-identimise süsteemidena.

(15) Olemasolevate teavitamis- ja vastastikuse hindamise menetluste ühtlustamine hoiab ära erinevate teavitatud e-identimise süsteemide ebaühtlase hindamise ja hõlbustab usalduse suurendamist liikmesriikide vahel. Uued lihtsustatud mehhanismid peaksid edendama liikmesriikide koostööd nende teavitatud e-identimise süsteemide turvalisuse ja koostalitlusvõime valdkonnas.

(16) Liikmesriikidel peaksid olema uued paindlikud vahendid, et tagada käesoleva määruse ja asjakohaste rakendusaktide nõuete täitmine. Käesolev määrus peaks võimaldama liikmesriikidel kasutada akrediteeritud vastavushindamisasutuste koostatud aruandeid ja hinnanguid, mis on ette nähtud määruse (EL) 2019/881 alusel liidu tasandil kehtestatavate sertifitseerimise kavadega, et toetada oma väiteid selle kohta, et kavad või nende osad on kooskõlas teavitatud e-identimise süsteemide koostalitlusvõimet ja turvalisust käsitlevate määruse nõuetega.

[7] Euroopa Parlamendi ja nõukogu 20. juuni 2019. aasta määrus (EL) 2019/1157 liidu kodanike isikutunnistuste ning vaba liikumise õigust kasutavatele liidu kodanikele ja nende pereliikmetele väljaantavate elamislubade turvalisuse suurendamise kohta (ELT L 188, 12.7.2019, lk 67).

(17a) Liikmesriikide väljastatud või Euroopa digiidentiteeditasku loodud kordumatute ja püsivate identifikaatorite kasutamine koos isikutuvastusandmete kasutamisega on oluline, et tagada kasutaja isikusamasuse kontrollimine, eelkõige avalikus sektoris ja kui see on ette nähtud liikmesriigi või liidu õigusega. Käesoleva määrusega tuleks tagada, et Euroopa digiidentiteeditaskuga kaasneb mehhanism andmete kokkulangevuse tagamiseks, sealhulgas kvalifitseeritud elektrooniliste atribuutide tõendite abil, ning sellega võimaldatakse kordumatute ja püsivate identifikaatorite lisamist isikutuvastusandmete kogumisse. Kordumatu ja püsiv identifikaator võib koosneda kas ühest või mitmest isikutuvastusandmeüksusest, mis võivad olla sektoripõhised, tingimusel et need võimaldavad kasutajat kogu liidus üheselt tuvastada. Euroopa digiidentiteeditasku peaks pakkuma ka mehhanismi, mis võimaldab kasutada tugineva isiku spetsiifilisi identifikaatoreid juhtudel, kui liikmesriigi või liidu õiguse kohaselt on nõutav kordumatu ja püsiva identifikaatori kasutamine. Igal juhul peaks andmete kokkulangevuse tagamise ning kordumatute ja püsivate identifikaatorite kasutamise hõlbustamiseks ette nähtud mehhanism tagama, et kasutaja on vastavalt käesolevale määrusele ja kohaldatavale liidu õigusele, eelkõige määrusele (EL) 2016/679, kaitstud isikuandmete väärkasutamise eest, sealhulgas profiilianalüüsi ja jälgimise riski eest seoses Euroopa digiidentiteeditasku kasutamisega.

(17aa) Oluline on võtta arvesse kasutajate vajadusi, suurendades seeläbi nõudlust Euroopa digiidentiteeditaskute järele. Euroopa digiidentiteeditaskutega seoses tuleks pakkuda sisukaid kasutusmalle ja digiidentiteeditaskutele tuginevaid internetipõhiseid teenuseid. Kasutajate mugavuse huvides ja selliste teenuste piiriülese kättesaadavuse tagamiseks on oluline võtta meetmeid, et soodustada sarnase lähenemisviisi kohaldamist internetipõhiste teenuste kavandamise, arendamise ja rakendamise suhtes kõigis liikmesriikides. Selle eesmärgi saavutamiseks võiks olla kasu mittesiduvatest suunistest Euroopa digiidentiteeditaskutel põhinevate internetipõhiste teenuste kavandamise, arendamise ja rakendamise kohta. Selliste suuniste koostamisel tuleks nõuetekohaselt arvesse võtta liidu koostalitlusvõime raamistikku. Liikmesriikidel peaks olema suuniste vastuvõtmisel juhtroll.

(18) Kooskõlas direktiiviga (EL) 2019/882[8] peaksid puuetega inimesed saama kasutada Euroopa digiidentiteeditaskuid, usaldusteenuseid ja nende teenuste osutamisel kasutatavaid lõpptarbijale suunatud tooteid teiste kasutajatega võrdsetel alustel.

(19) Käesolev määrus ei peaks 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.

(20) Usaldusteenuste osutamine ja kasutamine muutub rahvusvahelises kaubanduses ja koostöös üha olulisemaks. ELi rahvusvahelised partnerid loovad määrusest (EL) nr 910/2014 lähtuvaid usaldusraamistikke. Seega võib selliste teenuste ja nende osutajate tunnustamise hõlbustamiseks sätestada rakendusaktides tingimused, mille alusel võib kolmandate riikide usaldusraamistikke pidada samaväärseks käesolevas määruses sätestatud kvalifitseeritud usaldusteenuste ja nende osutajate usaldusraamistikuga, täiendamaks võimalust liidus ja kolmandates riikides asutatud usaldusteenuste ja nende osutajate vastastikuseks tunnustamiseks kooskõlas aluslepingu artikliga 218. Kui kehtestatakse tingimused, mille alusel võib kolmandate riikide usaldusraamistikke pidada samaväärseks käesolevas määruses sätestatud kvalifitseeritud usaldusteenuste ja teenuseosutajate usaldusraamistikuga, tuleks tagada ka vastavus direktiivi XXXX/XXXX (NIS2 direktiiv) ja määruse (EL) 2016/679 asjakohastega sätetega ning usaldusnimekirjade kui usalduse loomise oluliste elementide kasutamine.

---

[8] Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta direktiiv (EL) 2019/882 toodete ja teenuste ligipääsetavusnõuete kohta (ELT L 151, 7.6.2019, lk 70).

(21) Käesolev määrus peaks tuginema liidu õigusaktidele, millega tagatakse konkurentsile avatud ja õiglased turud digisektoris. Eelkõige tugineb see määrusele (EL) 2022/1925, millega kehtestatakse eeskirjad põhiplatvormiteenuse osutajatele ning muu hulgas keelatakse pääsuvalitsejatel nõuda ärikasutajatelt, et nad kasutaksid või pakuksid pääsuvalitseja identimisteenust või teeksid sellega koostööd, kui ärikasutajad pakuvad oma teenuseid kõnealuse pääsuvalitseja põhiplatvormiteenuseid kasutades. Määruse (EL) 2022/1925 artikli 6 lõike 7 kohaselt peavad kontrollijad võimaldama ärikasutajatele ja kõrvalteenuste osutajatele juurdepääsu samadele operatsioonisüsteemi, riist- või tarkvaraelementidele ning tagama samal tasemel koostalitlusvõime, mis on tagatud või mida kasutatakse pääsuvalitseja kõrvalteenuste osutamise korral. Digiturgude määruse artikli 2 punkti 15 kohaselt on identimisteenused kõrvalteenuste liik. Ärikasutajatel ja kõrvalteenuste osutajatel peaks seetõttu olema juurdepääs sellistele riist- või tarkvaraelementidele, näiteks nutitelefonide turvaelementidele, ning võimalus tagada nendega koostalitlus Euroopa digiidentiteeditaskute või liikmesriikide teavitatud e-identimise vahendite kaudu.

(22) Et ühtlustada usaldusteenuse osutajatele pandud küberturvalisuse kohustusi ning võimaldada teenuseosutajatel ja nende vastavatel pädevatel asutustel kasutada direktiiviga XXXX/XXXX (NIS2 direktiiv) kehtestatud õigusraamistikku, peavad usaldusteenuse osutajad võtma direktiivi XXXX/XXXX (NIS2 direktiiv) kohaselt asjakohaseid tehnilisi ja korralduslikke meetmeid, näiteks võtma meetmeid süsteemirikete, inimliku eksimuse, pahatahtliku tegevuse või loodusnähtuste käsitlemiseks, et juhtida riske, mis ohustavad nende üksuste teenuste osutamisel kasutatavate võrgu- ja infosüsteemide turvalisust, ning teatama olulistest intsidentidest ja küberohtudest kooskõlas direktiiviga XXXX/XXXX (NIS2 direktiiv). Usaldusteenuse osutajad peaksid teatama kõikidest intsidentidest, millel on oluline mõju nende teenuste osutamisele, sealhulgas sellistest intsidentidest, mis on põhjustatud seadmete vargusest või kaotsiminekust, võrgukaabli kahjustustest ning isiku tuvastamise käigus toimunud turvaintsidentidest. Direktiivi XXXXXX [NIS2 direktiiv] kohaseid küberturvalisuse riskijuhtimisnõudeid ja teatamiskohustusi tuleks käsitada käesoleva määruse alusel usaldusteenuse osutajate suhtes kehtestatud nõuete täiendusena. Direktiivi XXXX/XXXX (NIS2 direktiiv) kohaselt määratud pädevad asutused peaksid vajaduse korral jätkuvalt kohaldama väljakujunenud riiklikke tavasid või suuniseid seoses turva- ja aruandlusnõuete rakendamisega ning selliste nõuete täitmise järelevalvega vastavalt määrusele (EL) nr 910/2014. Käesolevas määruses sätestatud nõuded ei piira kohustust teatada isikuandmetega seotud rikkumistest vastavalt määrusele (EL) 2016/679.

(23) Nõuetekohast tähelepanu tuleks pöörata tõhusa koostöö tagamisele võrgu- ja infoturbeasutuste ning eIDASe asutuste vahel. Juhul kui käesoleva määruse kohane järelevalveasutus erineb direktiivi XXXX/XXXX [NIS2 direktiiv] alusel määratud pädevatest asutustest, peaksid need asutused tegema aegsasti tihedat koostööd, vahetades asjakohast teavet, et tagada tulemuslik järelevalve ja usaldusteenuse osutajate vastavus käesolevas määruses ja direktiivis XXXX/XXXX [NIS2 direktiiv] sätestatud nõuetele. Eelkõige peaks käesoleva määruse kohastel järelevalveasutustel olema õigus nõuda direktiivi XXXXX/XXXX [NIS2 direktiiv] kohaselt pädevalt asutuselt, et ta esitaks kvalifitseeritud staatuse andmiseks vajaliku asjakohase teabe ja võtaks järelevalvemeetmeid, et kontrollida, kas usaldusteenuse osutajad täidavad võrgu- ja infoturbe NIS2 direktiivi asjakohaseid nõudeid, või nõuda, et nad kõrvaldaksid mittevastavuse.

(24) 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. Selle tagamiseks, et kvalifitseeritud registreeritud e-andmevahetusteenust kasutades edastatakse andmed õigele adressaadile, peaksid kvalifitseeritud registreeritud e-andmevahetusteenused tagama adressaadi identimise täieliku kindlusega, samal ajal kui saatja identimiseks piisaks kõrgest usaldusväärsusest. Liikmesriigid peaksid julgustama kvalifitseeritud registreeritud e-andmevahetusteenuste osutajaid tagama oma teenuste koostalitlusvõime teiste kvalifitseeritud usaldusteenuse osutajate osutatavate kvalifitseeritud registreeritud e-andmevahetusteenustega, et elektrooniliselt registreeritud andmeid ladusalt kahe või enama kvalifitseeritud usaldusteenuse osutaja vahel edastada ja siseturul õiglasi tavasid edendada.

(25) Enamikul juhtudel ei ole kodanikel ja muudel elanikel turvalist ja kõrgetasemelist andmekaitset tagavat piiriülest võimalust vahetada digitaalselt sellist oma identiteediga seotud teavet nagu aadress, vanus ja kutsekvalifikatsioon, juhiload ja muud load ning makseandmed.

(26) Peaks olema võimalik väljastada ja hallata usaldusväärseid digitaalseid atribuute ning aidata vähendada halduskoormust, andes kodanikele ja muudele elanikele võimaluse kasutada neid oma era- ja avaliku sektori tehingutes. Kodanikel ja muudel elanikel peaks näiteks olema võimalik tõendada, et neil on ühe liikmesriigi ametiasutuse väljastatud kehtiv juhiluba, mida teiste liikmesriikide asjaomased ametiasutused saavad kontrollida ja millele nad võivad tugineda, ning kasutada piiriüleses kontekstis oma sotsiaalkindlustusõigusi või tulevasi elektroonilisi reisidokumente.

(27) Igal üksusel, kes kogub, loob ja väljastab tõendatud atribuute, nagu diplomid, litsentsid ja sünnitunnistused, peaks olema võimalus saada atribuutide elektroonilise tõendamise teenuse pakkujaks. Tuginevad isikud peaksid kasutama elektroonilisi atribuutide tõendeid samaväärsena paberkandjal tõenditega. Seega ei tohiks atribuutide elektroonilist tõendit tunnistada õiguslikult kehtetuks seetõttu, et see on elektroonilisel kujul või ei vasta kvalifitseeritud elektroonilistele atribuutide tõenditele esitatavatele nõuetele. Selleks tuleks sätestada üldnõuded, millega tagatakse, et kvalifitseeritud elektroonilisel atribuutide tõendil on seaduslikult väljastatud paberkandjal tõenditega samaväärne õiguslik toime. Neid nõudeid tuleks siiski kohaldada, ilma et see piiraks selliste liidu või siseriiklike õigusaktide kohaldamist, millega määratakse kindlaks täiendavad vormiga seotud sektoripõhised nõuded, millel on õiguslik toime, ja eelkõige atribuutide kvalifitseeritud elektrooniliste tõendite piiriülest tunnustamist, kui see on asjakohane.

(28) Euroopa digiidentiteeditaskute laialdase kättesaadavuse ja kasutatavuse tingimus on nende aktsepteerimine erasektori teenuseosutajate poolt. Erasektori tuginevad isikud, kes osutavad teenuseid transpordi, energia, panganduse, finantsteenuste, sotsiaalkindlustuse, tervishoiu, joogivee, postiteenuste, digitaristu, hariduse või telekommunikatsiooni valdkonnas, peaksid aktsepteerima Euroopa digiidentiteeditaskute kasutamist selliste teenuste osutamisel, mille puhul nõutakse siseriiklike või liidu õigusaktide või lepinguliste kohustuste alusel tugevat kasutaja autentimist. Euroopa digiidentiteeditasku kasutamise ja aktsepteerimise hõlbustamiseks tuleks arvesse võtta laialdaselt tunnustatud valdkondlikke standardeid ja spetsifikatsioone. Kui määruse [digiteenuste määruse viide] artikli 25 lõikes 1 määratletud väga suured digiplatvormid nõuavad kasutajate autentimist juurdepääsuks internetipõhistele teenustele, peaks neil platvormidel olema kohustus aktsepteerida kasutaja soovi korral Euroopa digiidentiteeditaskute kasutamist. Kasutajatel ei tohiks olla kohustust kasutada digitaskut erateenustele juurdepääsuks, kuid kui nad seda soovivad, peaksid suured digiplatvormid aktsepteerima sel eesmärgil Euroopa digiidentiteeditaskut, järgides samas võimalikult väheste andmete kogumise põhimõtet. Võttes arvesse, kui tähtsat rolli mängivad väga suured digiplatvormid nende haardeulatuse tõttu, mis väljendub eelkõige teenusesaajate ja majandustehingute hulgas, on see vajalik, et suurendada kasutajate kaitset pettuste eest ja tagada kõrgetasemeline andmekaitse. Välja tuleks töötada iseregulatsiooni tegevusjuhendid (edaspidi „tegevusjuhendid“), et aidata kaasa e-identimise vahendite (sealhulgas käesoleva määruse kohaldamisalasse kuuluvate Euroopa digiidentiteeditaskute) laialdasele kättesaadavusele ja kasutatavusele. Tegevusjuhendid peaksid hõlbustama e-identimise vahendite, sealhulgas Euroopa digiidentiteeditaskute laialdast aktsepteerimist selliste teenuseosutajate poolt, kes ei kvalifitseeru väga suurteks digiplatvormideks ja kes kasutavad kasutajate autentimiseks kolmandate isikute e-identimise teenuseid. Need tuleks välja töötada 12 kuu jooksul alates käesoleva määruse vastuvõtmisest. Komisjon peaks hindama nende sätete tõhusust Euroopa digiidentiteeditaskute kättesaadavuse ja kasutatavuse seisukohast 24 kuud pärast nende kasutuselevõttu.

(29) Valikuline avalikustamine on kontseptsioon, mis annab andmete omanikule õiguse avalikustada ainult osa suuremast andmekogumist, et andmeid saav üksus saaks ainult sellist teavet, mis on vajalik näiteks selleks, et kasutaja avaldaks tuginevale isikule ainult selliseid andmeid, mis on vajalikud kasutaja soovitud teenuse osutamiseks. Euroopa digiidentiteeditasku peaks tehniliselt võimaldama atribuutide valikulist avalikustamist tuginevatele isikutele. Selliseid valikuliselt avalikustatud atribuute, sealhulgas siis, kui algselt mitme eraldiseisva elektroonilise tõendi osad, võib hiljem kombineerida ja tuginevatele isikutele esitada. See funktsioon peaks muutuma põhiomaduseks, mis suurendab mugavust ja isikuandmete kaitset, sealhulgas tagab võimalikult väheste andmete kogumise.

(30) Kvalifitseeritud usaldusteenuse osutajate poolt kvalifitseeritud atribuudi tõendi osana pakutavaid atribuute peaksid autentsetest allikatest kontrollima kas otse kvalifitseeritud usaldusteenuse osutajad või tuleks selleks kasutada määratud vahendajaid, kes on vastavalt siseriiklikule või liidu õigusele tunnustatud selleks, et teostada tõendatud atribuutide turvalist vahetamist autentimisteenuse või atribuudi tõendamise teenuse pakkujate ja tuginevate isikute vahel. Liikmesriigid peaksid riiklikul tasandil kehtestama asjakohased mehhanismid tagamaks, et kvalifitseeritud elektroonilist atribuutide tõendit väljastavad kvalifitseeritud usaldusteenuse osutajad saavad selle isiku nõusolekul, kellele tõend on väljastatud, kontrollida atribuutide autentsust, tuginedes autentsetele allikatele. Asjakohased mehhanismid võivad hõlmata konkreetsete vahendajate või tehniliste lahenduste kasutamist kooskõlas siseriikliku õigusega, mis võimaldab juurdepääsu autentsetele allikatele. Sellise mehhanismi kättesaadavuse tagamine, mis võimaldab atribuutide kontrollimist autentsete allikate alusel, peaks hõlbustama kvalifitseeritud elektrooniliste atribuutide tõenditega tegelevate kvalifitseeritud usaldusteenuse osutajate poolt käesolevas määruses sätestatud kohustuste täitmist. VI lisa sisaldab nende atribuutide kategooriate loetelu, mille puhul liikmesriigid peaksid tagama, et võetakse meetmeid, mis võimaldavad kvalifitseeritud elektrooniliste atribuutide tõendite pakkujatel kasutaja taotlusel kontrollida elektrooniliselt nende autentsust asjakohase autentse allika alusel. Liikmesriigid peaksid kokku leppima nendesse kategooriatesse kuuluvates konkreetsetes atribuutides.

(31) Turvaline e-identimine ja atribuutide tõendamine peaks pakkuma finantsteenuste sektorile täiendavat paindlikkust ja lahendusi, mis võimaldavad identida kliente ja vahetada konkreetseid atribuute, mis on vajalikud näiteks selleks, et täita rahapesu tõkestamise määruse kohaseid kliendi suhtes rakendatavate hoolsusmeetmete nõudeid [viide lisatakse pärast ettepaneku vastuvõtmist], investorite kaitset käsitlevatest õigusaktidest tulenevaid sobivusnõudeid, või selleks, et makseteenuste valdkonnas toetada kontole sisselogimise ja tehingute algatamise eesmärgil toimuva e-identimise puhul kliendi tugeva autentimise nõuete täitmist.

(31a) Sertifitseerimistavade järjepidevuse tagamiseks kogu ELis peaks komisjon välja andma suunised kvalifitseeritud e-allkirja andmise vahendite ja kvalifitseeritud e-templi loomise vahendite sertifitseerimise ja uuesti sertifitseerimise kohta, sealhulgas nende kehtivuse ja ajaliste piirangute kohta. Käesolev määrus ei takista liikmesriike lubamast avalik-õiguslikel või eraõiguslikel asutustel, kellel on sertifitseeritud kvalifitseeritud e-allkirja andmise vahendid, ajutiselt pikendada sertifitseerimise kehtivust, kui sama seadet ei ole võimalik õiguslikult kindlaks määratud aja jooksul uuesti sertifitseerida muul põhjusel kui rikkumise või turvaintsidendi korral, ilma et see piiraks kohaldatavat sertifitseerimistava.

(32) Veebisaidi autentimisteenused tagavad kasutajatele kõrgel usaldusväärsuse tasemel, et veebisaiti käitab ehtne ja seaduslik üksus sõltumata sellest, mis platvormil seda kuvatakse. Need teenused aitavad suurendada usaldust ja kindlustunnet internetis toimuva äritegevuse suhtes ning vähendada võrgupettusi. Veebisaidi autentimisteenuste kasutamine peaks veebisaitide jaoks olema vabatahtlik. Selleks aga, et veebisaidi autentimisest saaks usalduse suurendamise, kasutajakogemuse parandamise ja majanduskasvu edendamise vahend siseturul, tuleks käesoleva määrusega kehtestada veebisaidi autentimisteenuse osutajatele ja nende teenustele minimaalsed turvalisuse ja vastutusega seotud kohustused. Selleks peaksid veebibrauserite pakkujad tagama toetuse ja koostalitlusvõime veebisaidi autentimise kvalifitseeritud sertifikaatidega vastavalt määrusele (EL) nr 910/2014. Nad peaksid tunnustama veebisaidi autentimise kvalifitseeritud sertifikaate ja võimaldama sertifitseeritud identiteediandmete kuvamist lõppkasutajale brauseri keskkonnas käesoleva määruse kohaselt kehtestatud spetsifikatsioonide alusel. Veebisaidi autentimise kvalifitseeritud sertifikaadi tunnustamine kvalifitseeritud sertifikaadina, mille on välja andnud kvalifitseeritud usaldusteenuse osutaja, peaks tagama, et sertifikaadis sisalduvaid identiteediandmeid on võimalik käesoleva määruse kohaselt autentida ja kontrollida. See ei tohiks mõjutada veebibrauserite pakkujate võimalust tegeleda oluliste mittevastavustega, mis on seotud üksiksertifikaatide turvalisuse rikkumise ja tervikluse kadumisega, aidates seeläbi kaasa lõppkasutajate turvalisusele internetis. Et kodanikke paremini kaitsta ja veebisaidi autentimise kvalifitseeritud sertifikaatide kasutamist veelgi edendada, peaksid liikmesriikide ametiasutused kaaluma nende lisamist oma veebisaitidele.

(33) Paljud liikmesriigid on kehtestanud riiklikud nõuded turvalise ja usaldusväärse digitaalse arhiveerimise teenustele, et võimaldada elektrooniliste andmete ja nendega seotud usaldusteenuste pikaajalist säilitamist. Õiguskindluse, usalduse ja ühtlustamise tagamiseks kõigis liikmesriikides tuleks kehtestada kvalifitseeritud elektroonilise arhiveerimise teenuste õigusraamistik, mis oleks inspireeritud muude käesolevas määruses sätestatud usaldusteenuste raamistikust. See raamistik peaks pakkuma usaldusteenuse osutajatele ja kasutajatele tõhusat töövahendit, mis sisaldab elektroonilise arhiveerimise teenuse funktsionaalseid nõudeid ja kvalifitseeritud elektroonilise arhiveerimise teenuse kasutamisest tulenevaid selgeid õiguslikke tagajärgi. Neid sätteid tuleks kohaldada nii elektrooniliselt koostatud dokumentide kui ka skaneeritud ja digiteeritud paberdokumentide suhtes. Vajaduse korral peaksid need sätted võimaldama konserveeritud elektrooniliste andmete portimist eri andmekandjatele või vormingutele, et pikendada nende püsivust ja loetavust kauemaks kui nende tehnoloogiline kehtivusaeg, minimeerides samal ajal võimalikult suures ulatuses andmete kaotsiminekut ja muutmist. Kui digitaalse arhiveerimise teenusele esitatud elektroonilised andmed sisaldavad ühte või mitut kvalifitseeritud e-allkirja või kvalifitseeritud e-templit, peaks teenus kasutama menetlusi ja tehnoloogiaid, millega on võimalik pikendada nende usaldusväärsust selliste andmete säilitusaja jooksul, tuginedes võimaluse korral muude käesoleva määrusega loodud kvalifitseeritud elektrooniliste usaldusteenuste kasutamisele. Säilitamistõendite loomiseks e-allkirjade, e-templite või e-ajatemplite kasutamise korral tuleks kasutada kvalifitseeritud elektroonilisi usaldusteenuseid. Liikmesriigid võivad elektroonilise arhiveerimise teenustega seoses käesolevas määruses ühtlustamata ulatuses ja kooskõlas liidu õigusega säilitada kõnealuseid teenuseid käsitlevad siseriiklikud sätted või neid kehtestada, näiteks erisätted, mis võimaldavad teha teatavaid erandeid teenuste puhul, mis on integreeritud organisatsiooni ja mida kasutatakse rangelt selle organisatsiooni „sisemiste arhiivide“ jaoks. Käesolevas määruses ei tohiks eristada elektrooniliselt koostatud dokumente ja digiteeritud füüsilisi dokumente.

(33a) Riiklikud arhiivid ja mäluasutused kui organisatsioonid, mis tegelevad dokumentaalpärandi säilitamisega avalikes huvides, on tavaliselt volitatud tegutsema siseriikliku õiguse alusel ning nad ei pruugi osutada usaldusteenuseid käesoleva määruse tähenduses. Kui need asutused selliseid teenuseid ei osuta, ei piira käesolev määrus nende toimimist.

(34) Elektroonilised registrid on elektrooniliste andmekirjete jada, mis tagab nende tervikluse ja kronoloogilise järjestuse täpsuse. Elektrooniliste registrite eesmärk on luua andmekirjete kronoloogiline järjestus, et hoida ära digitaalsete varade kopeerimist ja müümist mitmele saajale. Elektroonilisi registreid saab kasutada näiteks ülemaailmses kaubanduses omandiõiguse digitaalseks registreerimiseks, tarneahela rahastamiseks, intellektuaalomandi õiguste või kaupade, näiteks elektri digitaliseerimiseks. Koos muude tehnoloogiatega võivad need aidata leida lahendusi tõhusamateks ja ümberkujundavateks avalikeks teenusteks, nagu e-hääletamine, tolliasutuste piiriülene koostöö, akadeemiliste asutuste piiriülene koostöö või kinnisvara omandiõiguse registreerimine detsentraliseeritud kinnistusregistrites. Kvalifitseeritud elektroonilised registrid loovad õigusliku eelduse registri andmekirjete kordumatu ja täpse kronoloogilise järjestuse ja tervikluse suhtes. Elektrooniliste registrite konkreetsed atribuudid, st andmekirjete kronoloogiline järjestus, eristavad elektroonilisi registreid muudest usaldusteenustest, nagu e-ajatemplid ja registreeritud e-andmevahetusteenused. Nimelt ei saa digitaalsete dokumentide ajatempliga varustamine ega nende edastamine registreeritud e-andmevahetusteenuste abil ilma täiendavate tehniliste või korralduslike meetmeteta piisavalt ära hoida, et sama digitaalset vara kopeeritakse ja müüakse eri osapooltele rohkem kui üks kord. Elektroonilise registri loomise ja ajakohastamise protsess sõltub kasutatava (tsentraliseeritud või hajutatud) registri liigist.

(35) Et vältida siseturu killustumist, tuleks luua üleeuroopaline õigusraamistik, mis võimaldab andmete kvalifitseeritud elektroonilistes registritesse kandmiseks vajalike usaldusteenuste piiriülest tunnustamist. Elektrooniliste registrite usaldusteenuse osutajatele tuleks anda volitus teha kindlaks, et andmed kantakse registrisse järjestikku. Käesolevat määrust kohaldatakse olenemata mis tahes juriidilistest kohustustest, mida elektrooniliste registrite kasutajatel võib olla vaja täita liidu ja siseriikliku õiguse alusel. Näiteks isikuandmete töötlemisega seotud kasutusjuhud peavad olema kooskõlas määrusega (EL) 2016/679. Krüptovaradega seotud kasutusjuhud peaksid olema kooskõlas kõigi kohaldatavate finantsreeglitega, sealhulgas näiteks finantsinstrumentide turgude direktiiviga,[9] makseteenuste direktiiviga,[10] e-raha direktiiviga,[11] samuti võimalike tulevaste õigusaktidega krüptovaraturgude kohta ja rahapesuvastaste õigusnormidega, mis võidakse lisada rahaülekannete määrusesse,[12] ning millega võidakse nõuda, et krüptovarateenuse osutajad kontrolliksid elektrooniliste registrite kasutajate isikusamasust, et täita rahvusvahelisi rahapesuvastaseid standardeid.

---

9 Euroopa Parlamendi ja nõukogu 15. mai 2014. aasta direktiiv 2014/65/EL finantsinstrumentide turgude kohta ning millega muudetakse direktiivi 2002/92/EÜ (ELT L 173, 12.6.2014, lk 349–496).

10 Euroopa Parlamendi ja nõukogu 25. novembri 2015. aasta direktiiv (EL) 2015/2366 makseteenuste kohta siseturul, direktiivide 2002/65/EÜ, 2009/110/EÜ ning 2013/36/EL ja määruse (EL) nr 1093/2010 muutmise ning direktiivi 2007/64/EÜ kehtetuks tunnistamise kohta (ELT L 337, 23.12.2015, lk 35–127).

11 Euroopa Parlamendi ja nõukogu 16. septembri 2009. aasta direktiiv 2009/110/EÜ, mis käsitleb e-raha asutuste asutamist ja tegevust ning usaldatavusnormatiivide täitmise järelevalvet ning millega muudetakse direktiive 2005/60/EÜ ja 2006/48/EÜ ning tunnistatakse kehtetuks direktiiv 2000/46/EÜ (ELT L 267, 10.10.2009, lk 7–17).

12 Vt komisjoni 20. juuli 2021. aasta ettepanekut sõnastada uuesti Euroopa Parlamendi ja nõukogu määrus (EL) 2015/847, mis käsitleb rahaülekannetes ja teatavates krüptovaraülekannetes edastatavat teavet, COM/2021/422 final.

(36) Et vältida killustatust ja takistusi, mis tulenevad standardite lahknevusest ja tehnilistest piirangutest, ning tagada koordineeritud protsess, mis ei lase Euroopa tulevase digiidentiteedi raamistiku rakendamist ohtu seada, on vaja komisjoni, liikmesriikide ja erasektori tihedat ja struktureeritud koostööd. Selle eesmärgi saavutamiseks peaksid liikmesriigid tegema koostööd komisjoni soovituses XXX/XXXX [mis käsitleb ühiseid liidu tööriistu Euroopa digiidentiteedi raamistiku koordineeritud käsitlusviisi jaoks][13] sätestatud raamistikus, et määrata kindlaks Euroopa digiidentiteedi raamistiku tööriistad. Nende tööriistade hulka peaks kuuluma põhjalik tehniline arhitektuur ja võrdlusraamistik, ühiste standardite ja tehniliste viidete kogum ning juhiste ja heade tavade kirjelduste kogum, mis peaks hõlmama vähemalt Euroopa digiidentiteeditaskute, sealhulgas e-allkirjade, ning atribuutide tõendamise kvalifitseeritud usaldusteenuste funktsioonide ja koostalitlusvõime kõiki aspekte vastavalt käesolevas määruses sätestatule. Sellega seoses peaksid liikmesriigid jõudma kokkuleppele Euroopa digiidentiteeditaskute ärimudeli ja teenustasude struktuuri ühiste elementide suhtes, et hõlbustada nende kasutuselevõttu piiriülestes suhetes, eriti väikeste ja keskmise suurusega ettevõtetes. Tööriistad peaksid arenema paralleelselt Euroopa digiidentiteedi raamistiku üle peetava arutelu tulemuste ja raamistiku vastuvõtmise protsessiga ning neid kajastama.

(36a) Liikmesriigid peaksid kehtestama karistusnormid selliste rikkumiste puhuks nagu otsene või kaudne tegevus, mis põhjustab kvalifitseerimata ja kvalifitseeritud usaldusteenuste segiajamist või ELi usaldusmärgi kuritarvituslikku kasutamist kvalifitseerimata usaldusteenuse osutajate poolt. ELi usaldusmärki ei tohiks kasutada tingimustel, mis otseselt või kaudselt lasevad arvata, et mis tahes selle teenuseosutaja pakutavad kvalifitseerimata usaldusteenused on kvalifitseeritud.

[13] [lisada viide, kui soovitus on vastu võetud].

(36b) Käesoleva määrusega tuleks tagada kvalifitseeritud usaldusteenuste kvaliteedi, usaldusväärsuse ja turvalisuse ühtlustatud tase, olenemata sellest, kus neid toiminguid tehakse. Seega peaks kvalifitseeritud usaldusteenuse osutajal olema lubatud anda kvalifitseeritud usaldusteenuse osutamisega seotud toimingud edasi väljapoole liitu, kui ta esitab tagatised, millega kindlustatakse, et järelevalvetegevuse ja auditite läbiviimist saab tagada, justkui need toimingud oleksid tehtud liidus. Kui määruse järgimist ei ole võimalik täielikult tagada, peaks järelevalveasutustel olema võimalik võtta proportsionaalseid ja põhjendatud meetmeid, sealhulgas osutatavalt usaldusteenuselt kvalifitseeritud staatuse äravõtmine.

(36c) Kvalifitseeritud sertifikaadil põhinevate täiustatud e-allkirjade kehtivusega seotud õiguskindluse tagamiseks on väga oluline täpsustada, milliseid kvalifitseeritud sertifikaadil põhineva täiustatud e-allkirja osi peaks seda allkirja valideeriv tuginev isik hindama.

(36d) Usaldusteenuse osutajad peaksid kasutama krüptograafilisi algoritme, mis kajastavad praeguseid parimaid tavasid, ja nende algoritmide usaldusväärset rakendamist, et tagada oma usaldusteenuste turvalisus ja usaldusväärsus.

(36e) Käesolevas määruses tuleks sätestada kvalifitseeritud usaldusteenuse osutajate kohustus kontrollida selliste füüsiliste või juriidiliste isikute isikusamasust, kellele kvalifitseeritud sertifikaat on ELis väljastatud erinevate ühtlustatud meetodite alusel. Selline meetod võib hõlmata tuginemist e-identimise vahenditele, mis vastavad märkimisväärse usaldusväärsuse taseme nõuetele, koos täiendavate ühtlustatud kaugmenetlustega, mis tagavad isiku tuvastamise kõrge usaldusväärsusega.

(36f) Euroopa digiidentiteeditaskute väljastajaid ja teavitatud e-identimise vahendite väljastajaid, kes tegutsevad äri- või kutsetegevuse raames, kasutades pääsuvalitsejate pakutavaid põhiplatvormiteenuseid kaupade ja teenuste lõppkasutajatele pakkumise eesmärgil või selle käigus, tuleks käsitada ärikasutajatena vastavalt määruse (EL) 2022/1925 artikli 2 punktile 21. Seepärast tuleks pääsuvalitsejatelt nõuda, et nad tagaksid tasuta tõhusa koostalitlusvõime samade operatsioonisüsteemi, riist- või tarkvarafunktsioonidega, mis on kättesaadavad või mida kasutatakse pääsuvalitseja enda täiendavate ja tugiteenuste osutamisel ning riistvara pakkumisel, ning koostalitlusvõime eesmärgil juurdepääsu sellistele funktsioonidele. See peaks võimaldama Euroopa digiidentiteeditaskute väljastajatel ja teavitatud e-identimise vahendite väljastajatel ühenduda liideste või sarnaste lahenduste kaudu vastavate funktsioonidega sama tõhusalt kui pääsuvalitseja enda teenuste või riistvara kaudu.

(36g) Et tagada käesoleva määruse kooskõla praeguste arengusuundumustega ja järgida siseturu tavasid, tuleks komisjoni vastu võetud delegeeritud õigusaktid ja rakendusaktid korrapäraselt läbi vaadata ja vajaduse korral tuleks neid ajakohastada. Ajakohastamise vajalikkuse hindamisel tuleks arvesse võtta siseturul kasutusele võetud uusi tehnoloogiaid, tavasid, standardeid või tehnilisi kirjeldusi.

(37) Euroopa Andmekaitseinspektoriga konsulteeriti kooskõlas määruse (EL) 2018/1725[14] artikli 42 lõikega 1.

(38) Määrust (EL) 910/2014 tuleks seetõttu vastavalt muuta,

---

[14] Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39).

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Määrust (EL) nr 910/2014 muudetakse järgmiselt.

1) Artikkel 1 asendatakse järgmisega:

„Käesoleva määruse eesmärk on tagada siseturu nõuetekohane toimimine ning saavutada e-identimise vahendite ja usaldusteenuste asjakohane turvalisuse tase. Neil eesmärkidel käesolevas määruses:

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

ab) sätestatakse tingimused, mille alusel liikmesriigid pakuvad ja tunnustavad Euroopa digiidentiteeditaskuid;

b) sätestatakse usaldusteenuste, eelkõige e-tehingute eeskirjad,

c) kehtestatakse õigusraamistik e-allkirjade, e-templite, e-ajatemplite, e-dokumentide, registreeritud e-andmevahetusteenuste, veebisaidi autentimise sertifitseerimisteenuste, e-allkirjade, e-templite ja nende sertifikaatide elektroonilise valideerimise, veebisaidi autentimise sertifikaatide elektroonilise valideerimise, e-allkirjade, e-templite ja nende sertifikaatide elektroonilise säilitamise, elektroonilise arhiveerimise, atribuutide elektrooniliste tõendite, kvalifitseeritud e-allkirja vahemaa tagant andmise ja e-templi vahemaa tagant loomise vahendite haldamise ning elektrooniliste registrite jaoks.“

2) Artiklit 2 muudetakse järgmiselt:

a) lõige 1 asendatakse järgmisega:

„1. Käesolevat määrust kohaldatakse liikmesriikide poolt teavitatud e-identimise süsteemide, liikmesriikide poolt pakutavate Euroopa digiidentiteeditaskute ja liidus asuvate usaldusteenuse osutajate suhtes.“;

b) lõige 3 asendatakse järgmisega:

„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 või sektoripõhiste vorminõuetega.“

3) Artiklit 3 muudetakse järgmiselt:

X) punkt 1 asendatakse järgmisega:

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

a) punkt 2 asendatakse järgmisega:

„2) „e-identimise vahend“– kehaline ja/või kehatu üksus, sealhulgas Euroopa digiidentiteeditaskud, mis sisaldab isikutuvastusandmeid ja mida kasutatakse internetipõhiste või, kui see on asjakohane, ka internetiväliste teenuste puhul autentimiseks;“;

aa) punkt 3 asendatakse järgmisega:

„3) „isikutuvastusandmed“– liidu või siseriikliku õiguse kohaselt väljastatud andmed, mis võimaldavad teha kindlaks füüsilise või juriidilise isiku või füüsilist või juriidilist isikut esindava füüsilise isiku;“;

b) punkt 4 asendatakse järgmisega:

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

ba) punkt 5 asendatakse järgmisega:

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

bb) lisatakse järgmine punkt 5a:

5a) „kasutaja“ – füüsiline või juriidiline isik või füüsilist või juriidilist isikut esindav füüsiline isik, kes kasutab käesoleva määruse kohaselt pakutavaid usaldusteenuseid või e-identimise vahendeid;“;

c) punkt 14 asendatakse järgmisega:

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

d) punkt 16 asendatakse järgmisega:

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

a) e-allkirja sertifikaatide, e-templi sertifikaatide, veebisaidi autentimise sertifikaatide või muude usaldusteenuste osutamiseks vajalike sertifikaatide väljastamine;

aa) e-allkirja sertifikaatide, e-templi sertifikaatide, veebisaidi autentimise sertifikaatide või muude usaldusteenuste osutamiseks vajalike sertifikaatide valideerimine;

b) e-allkirjade või e-templite loomine;

c) e-allkirjade või e-templite valideerimine;

d) e-allkirjade, e-templite, e-allkirja sertifikaatide või e-templi sertifikaatide säilitamine;

e) kvalifitseeritud e-allkirja vahemaa tagant andmise ja e-templi vahemaa tagant loomise vahendite haldamine;

f) atribuutide elektrooniliste tõendite väljastamine;

fa) atribuutide elektrooniliste tõendite valideerimine;

g) e-ajatemplite loomine;

ga) e-ajatemplite valideerimine;

gb) registreeritud e-andmevahetusteenuste osutamine;

gc) registreeritud e-andmevahetusteenuste kaudu edastatud andmete ja nendega seotud tõendite valideerimine;

h) elektrooniliste andmete elektrooniline arhiveerimine; või

i) elektrooniliste andmete kandmine elektroonilisse registrisse;“;

da) punkt 18 asendatakse järgmisega:

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 või Euroopa digiidentiteeditaskute või e-identimise vahendite sertifitseerimist;“;

e) punkt 21 asendatakse järgmisega:

„21) „toode“– riist- või tarkvara või riist- ja/või tarkvara asjakohased osad, mis on ette nähtud e-identimise ja usaldusteenuste osutamiseks;“;

f) lisatakse punktid 23 a ja 23b:

„23a) „kvalifitseeritud e-allkirja vahemaa tagant andmise vahend“ – kvalifitseeritud e-allkirja andmise vahend, mida kvalifitseeritud usaldusteenuse osutaja haldab allkirja andja nimel vastavalt artiklile 29a;

„23b) „kvalifitseeritud e-templi vahemaa tagant loomise vahend“ – kvalifitseeritud e-templi loomise vahend, mida kvalifitseeritud usaldusteenuse osutaja haldab templi looja nimel vastavalt artiklile 39a;“;

g) punkt 29 asendatakse järgmisega:

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

h) punkt 41 asendatakse järgmisega:

„41) „valideerimine“ – protsess, mille käigus kontrollitakse ja kinnitatakse, et elektroonilised andmed on käesoleva määruse nõuete kohaselt kehtivad;“;

i) lisatakse punktid 42–55b:

„42) „Euroopa digiidentiteeditasku“ – e-identimise vahend, mis võimaldab kasutajal salvestada ja otsida identiteediandmeid, sealhulgas isikutuvastusandmeid ja nende identiteediga seotud atribuutide elektroonilisi tõendeid, esitada neid taotluse korral tuginevatele isikutele ning kasutada neid autentimiseks nii võrgus ning asjakohase juhul ka võrguväliselt teenuse jaoks kooskõlas artikliga 6a, ning mis võimaldab allkirjastada kvalifitseeritud e-allkirjaga ja kinnitada kvalifitseeritud e-templiga;

43) „atribuut“ – füüsilise või juriidilise isiku või eseme omadus, kvaliteet, õigus või luba;

44) „atribuutide elektrooniline tõend“ – elektrooniline tõend, mis võimaldab atribuute autentida;

45) „kvalifitseeritud elektrooniline atribuutide tõend“– atribuutide elektrooniline tõend, mille on väljastanud kvalifitseeritud usaldusteenuse osutaja ja mis vastab V lisas sätestatud nõuetele;

45a) „autentse teabeallika eest vastutava avaliku sektori asutuse poolt või nimel välja antud elektrooniline atribuutide tõend“ – atribuutide elektroonilised tõendid, mille on välja andnud autentse teabeallika eest vastutav avaliku sektori asutus või avaliku sektori asutus, kelle liikmesriik on määranud välja andma selliseid atribuutide tõendeid autentsete teabeallikate eest vastutavate avaliku sektori asutuste nimel kooskõlas artikliga 45da, ja mis vastavad VII lisas sätestatud nõuetele;

46) „autentne teabeallikas“ – avaliku sektori asutuse või eraõigusliku isiku vastutusel olev andmehoidla või süsteem, mis sisaldab ja pakub füüsilise või juriidilise isiku atribuute ja mida peetakse selle teabe peamiseks allikaks või mis on liidu või siseriikliku õiguse, sealhulgas haldustava kohaselt tunnustatud autentsena;

47) „elektrooniline arhiveerimine“ – teenus, millega tagatakse elektrooniliste andmete vastuvõtmine, säilitamine, otsimine ja kustutamine, et tagada nende säilimine ja loetavus ning säilitada nende terviklus, konfidentsiaalsus ja päritolutõend kogu säilitamisaja jooksul;

48) „kvalifitseeritud elektroonilise arhiveerimise teenus“– elektroonilise arhiveerimise teenus, mis vastab artiklis 45ga sätestatud nõuetele;

49) „ELi digiidentiteeditasku usaldusmärk“ – lihtsal, äratuntaval ja selgel viisil esitatud kontrollitav märge selle kohta, et Euroopa digiidentiteeditaskut pakutakse kooskõlas käesoleva määrusega;

50) „tugev kasutaja autentimine“ – autentimine, mille käigus kasutatakse vähemalt kahte erineva kategooria autentimistegurit, mis kuuluvad teadmise (miski, mida teab üksnes kasutaja), omamise (miski, mida omab üksnes kasutaja) või tunnuse (miski, mis on kasutajale omane) kategooriasse ja on sõltumatud, et neist ühe rikkumine ei ohustaks teiste usaldusväärsust, ning mille ülesehitus võimaldab kaitsta autentimisandmete konfidentsiaalsust;

53) „elektrooniline register“ – elektrooniliste andmekirjete jada, mis tagab nende tervikluse ja kronoloogilise järjestuse täpsuse;

53a) „kvalifitseeritud elektrooniline register“– elektrooniline register, mis vastab artiklis 45i sätestatud nõuetele;

54) „isikuandmed“ – igasugune määruse (EL) 2016/679 artikli 4 punktis 1 määratletud teave;

55) „andmete kokkulangevuse tagamine“ – protsess, mille käigus autentse teabeallika eest vastutava avaliku sektori asutuse poolt või nimel välja antud isikutuvastamisandmed, isiku identimise vahendid, kvalifitseeritud elektrooniline atribuutide tõend või atribuutide tõendid sobitatakse või lingitakse samale isikule kuuluva olemasoleva kontoga;

55a) „kordumatu ja püsiv identifikaator“ – identifikaator, mis võib koosneda ühest või mitmest riiklikust või sektoripõhisest isikutuvastamisandmeüksusest, on seotud ühe kasutajaga konkreetses süsteemis ja on ajaliselt püsiv;

55b) „andmekirje“ – elektroonilised andmed, mis on salvestatud koos seotud metaandmetega (või atribuutidega), mis toetavad andmete töötlemist;

55c) „Euroopa digiidentiteeditaskute võrguväline kasutamine“ – kasutaja ja tugineva isiku vaheline suhtlus füüsilises asukohas, mille puhul ei ole identiteeditaskul vaja suhtluse eesmärgil elektroonilise side võrkude kaudu kaugsüsteemidele juurde pääseda.“;

„*Artikkel 5*

Varjunimed e-tehingute tegemisel

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

5) II peatükki lisatakse artikli 6a ette järgmine peakiri:

„1. JAGU

Euroopa digiidentiteeditasku“.

7) Lisatakse artiklid 6a, 6b, 6c ja 6d:

„*Artikkel 6a*

Euroopa digiidentiteeditaskud

1. Tagamaks, et kõigil liidu füüsilistel ja juriidilistel isikutel on turvaline, usaldusväärne ja sujuv piiriülene juurdepääs avalikele ja erateenustele, tagab iga liikmesriik, et Euroopa digiidentiteeditaskut pakutakse 24 kuu jooksul pärast lõikes 11 ja artikli 6c lõikes 4 osutatud rakendusaktide jõustumist.

2. Euroopa digiidentiteeditaskut pakutakse:

   a) liikmesriigi poolt;

   b) liikmesriigi volituse alusel; või

   c) liikmesriigist sõltumatult, kuid liikmesriik tunnustab seda.

3. Euroopa digiidentiteeditaskud on e-identimise vahendid, mis võimaldavad kasutajal talle läbipaistval ja tema poolt jälgitaval viisil:

   a) turvaliselt taotleda, valida, kombineerida, salvestada, kustutada ja esitada tuginevatele isikutele atribuutide elektroonilisi tõendeid ja isikutuvastusandmeid, sealhulgas teostada autentimist võrgus ja asjakohasel juhul ka võrguväliselt, et kasutada avalikke ja erateenuseid, tagades samal ajal, et andmete valikuline avalikustamine on võimalik;

   b) allkirjastada kvalifitseeritud e-allkirjaga ja kinnitada kvalifitseeritud e-templiga.

4. Euroopa digiidentiteeditaskute eesmärk on eelkõige:

a) pakkuda ühiseid liideseid:

1) isikutuvastusandmete, kvalifitseeritud ja kvalifitseerimata elektrooniliste atribuutide tõendite või Euroopa digiidentiteeditasku kvalifitseeritud ja kvalifitseerimata sertifikaatide väljaandmiseks;

2) tuginevatele isikutele, et taotleda isikutuvastusandmeid ja atribuutide elektroonilisi tõendeid;

3) tuginevatele isikutele isikutuvastusandmete või atribuutide elektrooniliste tõendite esitamiseks võrgus ja asjakohasel juhul ka võrguväliselt;

4) kasutajale, et tal oleks võimalik suhelda Euroopa digiidentiteeditaskuga ja kuvada ELi digiidentiteeditasku usaldusmärki;

b) mitte anda atribuutide elektroonilisi tõendeid väljastavatele usaldusteenuse osutajatele mingit teavet nende atribuutide kasutamise kohta pärast nende väljastamist;

ba) tagada, et tuginevate isikute isikusamasust saab kontrollida, rakendades autentimise mehhanisme kooskõlas artikliga 6b;

c) täita artiklis 8 sätestatud nõudeid seoses kõrge usaldusväärsuse tasemega, mida kohaldatakse mutatis mutandis isikutuvastusandmete haldamise ja kasutamise suhtes digiidentiteeditasku kaudu, sealhulgas e-identimise ja e-autentimise suhtes;

e) tagada, et artikli 12 lõike 4 punktis d osutatud isikutuvastamisandmed tähistavad üheselt ja püsivalt digiidentiteeditaskuga seotud füüsilist isikut, juriidilist isikut või füüsilist isikut, kes esindab füüsilist isikut või juriidilist isikut.

4a Liikmesriigid näevad ette menetlused, mis võimaldavad kasutajal teatada oma digiidentiteeditasku võimalikust kaotsiminekust või väärkasutamisest ning taotleda selle tühistamist.

5. Liikmesriigid näevad ette Euroopa digiidentiteeditaskute valideerimismehhanismid, et:

a) tagada võimalus selle autentsust ja kehtivust kontrollida;

d) võimaldada kasutajal autentida tuginevaid isikuid vastavalt artiklile 6b.

6. Euroopa digiidentiteeditaskud väljastatakse teavitatud kõrge usaldusväärsuse tasemega e-identimise süsteemi alusel.

6a Euroopa digiidentiteeditaskute väljastamine, autentimiseks kasutamine ja tühistamine on füüsilistele isikutele tasuta.

6b Ilma et see piiraks artikli 6db kohaldamist, võivad liikmesriigid kooskõlas siseriikliku õigusega näha ette Euroopa digiidentiteeditaskute lisafunktsioonid, sealhulgas koostalitlusvõime olemasolevate riiklike e-identimise vahenditega.

7. Kasutajatel on täielik kontroll Euroopa digiidentiteeditasku ja nende Euroopa digiidentiteeditaskus sisalduvate andmete kasutamise üle. Euroopa digiidentiteeditasku väljastaja ei kogu digitasku kasutamise kohta teavet, mis ei ole vajalik teenuse osutamiseks, ega ühenda isikutuvastusandmeid ja muid Euroopa digiidentiteeditasku kasutamisega seotud või salvestatud isikuandmeid isikuandmetega, mis pärinevad selle väljastaja pakutavatest muudest teenustest või kolmandate isikute pakutavatest teenustest, mis ei ole vajalikud teenuse osutamiseks, välja arvatud juhul, kui kasutaja on seda sõnaselgelt taotlenud. Euroopa digiidentiteeditaskute pakkumisega seotud isikuandmeid hoitakse loogiliselt lahus kõigist muudest andmetest, mida Euroopa digiidentiteeditaskute väljastaja säilitab. Kui Euroopa digiidentiteeditaskuid pakuvad eraõiguslikud isikud vastavalt lõike 2 punktidele b–c, kohaldatakse artikli 45f lõike 4 sätteid *mutatis mutandis*.

7a. Liikmesriigid edastavad komisjonile põhjendamatu viivituseta teabe järgmise kohta:

a) asutus, kes vastutab Euroopa digiidentiteeditaskutele tuginevate teavitatud tuginevate isikute nimekirja koostamise ja haldamise eest vastavalt artikli 6b lõikega 2;

b) asutused, kes vastutavad Euroopa digiidentiteeditaskute pakkumise eest vastavalt artikli 6a lõikele 1;

c) asutused, kes vastutavad selle tagamise eest, et isikutuvastamisandmed on seotud digiidentiteeditaskuga vastavalt artikli 6a lõike 4 punktile e.

Teates esitatakse ka teave mehhanismi kohta, mis võimaldab artikli 12 lõikes 4 osutatud isikutuvastamisandmeid ja tuginevate isikute identiteeti valideerida.

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

8. Artiklit 11 kohaldatakse Euroopa digiidentiteeditasku suhtes *mutatis mutandis*.

9. Artikli 24 lõike 2 punkte b, e, g ja h kohaldatakse mutatis mutandis Euroopa digiidentiteeditaskute väljastaja suhtes.

10. Euroopa digiidentiteeditasku tehakse puuetega inimestele kättesaadavaks vastavalt direktiivis 2019/882 sätestatud ligipääsetavusnõuetele.

11. Kuue kuu jooksul pärast käesoleva määruse jõustumist määrab komisjon kindlaks lõigetes 3, 4, 5 ja 7a osutatud nõuete tehnilised kirjeldused ja tegevusspetsifikatsioonid ning võrdlusstandardid, võttes vastu rakendusakti Euroopa digiidentiteeditaskute teostamise kohta. Kõnealune rakendusakt võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

11a. Komisjon kehtestab tehnilised kirjeldused ja tegevusspetsifikatsioonid ning võrdlusstandardid, et hõlbustada Euroopa digiidentiteeditasku kasutajaks registreerimist, kasutades kas kõrgele usaldusväärsuse tasemele vastavaid e-identimise vahendeid või märkimisväärsele usaldusväärsuse tasemele vastavaid e-identimise vahendeid koos täiendavate kaugregistreerimismenetlustega, mis üheskoos vastavad kõrge usaldusväärsuse taseme nõuetele. Kõnealune rakendusakt võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 6b

Tuginevad isikud seoses Euroopa digiidentiteeditaskutega

1. Kui tuginevad isikud, kes osutavad era- või avalikke teenuseid, kavatsevad tugineda käesoleva määruse kohaselt pakutavatele Euroopa digiidentiteeditaskutele, teavitavad nad sellest liikmesriiki, kus asjaomased tuginevad isikud on asutatud.

1a Teavitamismenetlus peab olema kulutõhus ja riski suhtes proportsionaalne ning tagama, et tuginevad isikud esitavad vähemalt Euroopa digiidentiteeditaskutele autentimiseks vajaliku teabe. See peaks hõlmama vähemalt liikmesriiki, kus nad on asutatud, ja tugineva isiku nime ning asjakohasel juhul ametlikes dokumentides esitatud registreerimisnumbrit.

1b Teavitamisnõue ei piira muid liidu või siseriikliku õiguse kohaseid teavitamis- ja registreerimisnõudeid, näiteks isikuandmete eriliikide suhtes kohaldatavaid nõudeid, mille puhul võidakse nõuda täiendavaid loanõudeid/näiteks nõudeid, mida kohaldatakse isikuandmete eriliikide suhtes, mille puhul võib olla vaja täiendavaid loanõudeid.

1c Liikmesriigid võivad vabastada tuginevad isikud teavitamise nõudest, kui liidu või siseriiklikus õiguses ei ole ette nähtud konkreetseid teavitamis- või registreerimisnõudeid, et saada juurdepääs Euroopa digiidentiteeditasku kaudu esitatud teabele. Vabastatud tuginevatel isikutel ei pruugi olla vaja autentida Euroopa digiidentiteeditaskule.

1d Tuginevad isikud, keda on käesoleva artikli kohaselt teavitatud, teavitavad liikmesriiki viivitamata kõigist hilisematest muudatustest algselt esitatud teabes.

2. Tuginevad isikud tagavad artikli 6a lõike 4 punktis ba osutatud autentimismehhanismide rakendamise.

3. Tuginevad isikud vastutavad isikute autentimise menetluse ja Euroopa digiidentiteeditaskutest pärinevate ning ühise liidese kaudu artikli 6a lõike 4 punkti a alapunkti 2 kohaselt saadud atribuutide elektrooniliste tõendite valideerimise läbiviimise eest.

4. Kuue kuu jooksul pärast käesoleva määruse jõustumist määrab komisjon kindlaks lõigetes 1, 1a ja 1d osutatud nõuete tehnilised ja tegevusspetsifikatsioonid, võttes vastu artikli 6a lõikes 11 osutatud rakendusakti Euroopa digiidentiteeditaskute rakendamise kohta. Kõnealune rakendusakt võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 6c

Euroopa digiidentiteeditaskute sertifitseerimine

1. Euroopa digiidentiteeditaskute vastavust artikli 6a lõigetes 3, 4 ja 5 sätestatud nõuetele, artikli 6a lõikes 7 sätestatud loogilise eraldamise nõudele ja kohaldataval juhul artikli 6a lõikes 11a sätestatud nõuetele sertifitseerivad küberturvalisuse määruse artikli 60 kohaselt akrediteeritud vastavushindamisasutused ning seda tehakse ka lõike 4 punktide a, aa ja aaa kohaselt osutatud ja liikmesriikide määratud süsteemide, spetsifikatsioonide, standardite ja menetlustega. Sertifitseerimine kehtib kuni viis aastat, sõltuvalt korrapärasest nõrkuste hindamisest iga kahe aasta tagant. Kui tehakse kindlaks nõrkused ja neid ei kõrvaldata kolme kuu jooksul, sertifitseerimine tühistatakse.

2. Seoses artikli 6a lõike 7 kohaste andmekaitsenõuete täitmisega võib lõike 1 kohast sertifitseerimist täiendada määruse (EL) 2016/679 artikli 42 kohase sertifitseerimisega.

3. Euroopa digiidentiteeditaskute või nende osade vastavust artikli 6a lõigetes 3, 4, 5 ja 7 ning kohaldataval juhul lõikes 11a sätestatud küberturvalisuse seisukohast asjakohastele nõuetele sertifitseerivad lõikes 1 osutatud vastavushindamisasutused määruse (EL) 2019/881 kohaste asjakohaste küberturvalisuse sertifitseerimise kavade alusel, nagu neile on viidatud vastavalt lõike 4 punktile a ja lõike 4 punktile aa.

3a. Sertifitseeritud Euroopa digiidentiteeditaskute suhtes ei kohaldata artiklites 7 ja 9 osutatud nõudeid.

4. 6 kuu jooksul pärast käesoleva määruse jõustumist kehtestab komisjon rakendusaktidega:

a) loetelu määruse (EL) 2019/881 kohastest küberturvalisuse sertifitseerimise kavadest, mis on vajalikud Euroopa digiidentiteeditaskute sertifitseerimiseks, nagu on osutatud lõikes 3;

aa) spetsifikatsioonid, menetlused ja võrdlusstandardid nende kasutamiseks punkti a kohaselt loetletud asjakohaste küberturvalisuse sertifitseerimise kavade alusel;

aaa) loetelu spetsifikatsioonidest, menetlustest ja võrdlusstandarditest, millega lõikes 1 osutatud sertifitseerimise eesmärgil kehtestatakse ühised sertifitseerimisnõuded, mida määruse (EL) 2019/881 kohased asjakohased küberturvalisuse sertifitseerimise kavad ei hõlma, ning eesmärgiga näidata, et Euroopa digiidentiteeditasku vastab lõikes 1 osutatud nõuetele;

b) tehnilised kirjeldused, menetluslikud, organisatsioonilised ja tegevusspetsifikatsioonid lõikes 1 osutatud vastavushindamisasutuste määramiseks ning punkti aaa kohaselt kehtestatud sertifitseerimisnõuete puhul selliste sertifitseerimiskavade ja nendega seotud hindamismeetodite järelevalveks ja läbivaatamiseks, mida need asutused kasutavad, ning nende väljaantavate sertifikaatide ja sertifitseerimisaruannete järelevalveks ja läbivaatamiseks.

5. Liikmesriigid teatavad komisjonile lõikes 1 osutatud avalike või erasektori asutuste nimed ja aadressid. Komisjon teeb selle teabe liikmesriikidele kättesaadavaks.

6. Lõikes 4 osutatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 6d

Sertifitseeritud Euroopa digiidentiteeditaskute nimekirja avaldamine

1. Liikmesriigid teatavad komisjonile põhjendamatu viivituseta Euroopa digiidentiteeditaskutest, mida pakutakse artikli 6a kohaselt ja mis on sertifitseeritud artikli 6c lõikes 1 osutatud asutuste poolt. Samuti teatavad nad komisjonile põhjendamatu viivituseta sertifitseerimise tühistamisest.

2. Saadud teabe põhjal koostab komisjon sertifitseeritud Euroopa digiidentiteeditaskute masinloetava nimekirja, avaldab selle ja ajakohastab seda.

3. Kuue kuu jooksul pärast käesoleva määruse jõustumist määrab komisjon kindlaks lõigete 1 ja 2 kohaldamisega seotud formaadid ja menetlused, võttes vastu rakendusakti Euroopa digiidentiteeditaskute rakendamise kohta vastavalt artikli 6a lõikele 11. Kõnealune rakendusakt võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 6da

Euroopa digiidentiteeditaskute turvanõuete rikkumine

1. Kui artikli 6a kohaselt pakutavad Euroopa digiidentiteeditaskud ja artikli 6a lõike 5 punktides a, d või e osutatud valideerimismehhanismid murtakse või need on osaliselt rikutud viisil, mis mõjutab nende usaldusväärsust või muude Euroopa digiidentiteeditaskute usaldusväärsust, peatab asjaomaste digiidentiteeditaskute väljastaja põhjendamatu viivituseta Euroopa digiidentiteeditasku väljastamise ja kasutamise. Liikmesriik, kus asjaomaseid digiidentiteeditaskuid pakuti, teavitab sellest põhjendamatu viivituseta liikmesriike ja komisjoni. Asjaomaste digiidentiteeditaskute väljastaja või liikmesriik teavitab sellest tuginevaid isikuid ja kasutajaid.

2. Pärast lõikes 1 osutatud murde või rikkumise kõrvaldamist taastab digiidentiteeditasku väljastaja Euroopa digiidentiteeditasku väljastamise ja kasutamise. Liikmesriik, kus asjaomaseid digiidentiteeditaskuid pakuti, teavitab sellest põhjendamatu viivituseta liikmesriike ja komisjoni. Asjaomaste digiidentiteeditaskute väljastaja või liikmesriik teavitab sellest põhjendamatu viivituseta tuginevaid isikuid ja kasutajaid.

3. Kui lõikes 1 osutatud murret või rikkumist ei kõrvaldata kolme kuu jooksul alates peatamisest, tunnistab asjaomane liikmesriik kõnealuse Euroopa digiidentiteeditasku kehtetuks ning teavitab sellest teisi liikmesriike ja komisjoni. Kui rikkumise tõsidus seda õigustab, tunnistatakse asjaomane Euroopa digiidentiteeditasku põhjendamatu viivituseta kehtetuks.

4. Komisjon avaldab artiklis 6d osutatud nimekirjas tehtud muudatused põhjendamatu viivituseta *Euroopa Liidu Teatajas*.

5. Kuue kuu jooksul pärast käesoleva määruse jõustumist täpsustab komisjon lõigetes 1–3 osutatud meetmeid, võttes vastu artikli 6a lõikes 11 osutatud rakendusakti Euroopa digiidentiteeditaskute rakendamise kohta. Kõnealune rakendusakt võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 6db

Piiriülene tuginemine Euroopa digiidentiteeditaskutele

1. Kui liikmesriigid nõuavad avaliku sektori asutuse osutatavale internetipõhisele teenusele juurdepääsuks e-identimist e-identimise vahendi abil ja autentimist, aktsepteerivad nad kasutaja autentimise eesmärgil ka käesoleva määruse kohaselt pakutavaid Euroopa digiidentiteeditaskuid.

2. Kui teenuseid osutavad erasektori tuginevad isikud, välja arvatud komisjoni soovituses 2003/361/EÜ määratletud mikroettevõtjad ja väikeettevõtjad, peavad siseriiklike või liidu õigusaktide kohaselt kasutama e-identimise korral tugevat kasutaja autentimist või kui seda nõutakse lepinguliste kohustuste kohaselt, sealhulgas sellistes valdkondades nagu transport, energia, pangandus, finantsteenused, sotsiaalkindlustus, tervishoid, joogivesi, postiteenused, digitaristu, haridus või telekommunikatsioon, peavad erasektori tuginevad isikud hiljemalt 12 kuud pärast Euroopa digiidentiteeditaskute pakkumise kuupäeva vastavalt artikli 6a lõikele 1 ja rangelt kasutaja vabatahtliku taotluse korral, aktsepteerima ka käesoleva määruse kohaselt pakutavate Euroopa digiidentiteeditaskute kasutamist miinimumandmete puhul, mis on vajalikud konkreetse internetipõhise teenuse jaoks, mille jaoks taotletakse kasutaja autentimist.

3. Kui määruse [digiteenuste määruse viide] artikli 25 lõikes 1 määratletud väga suured digiplatvormid nõuavad kasutajate autentimist juurdepääsuks internetipõhistele teenustele, aktsepteerivad nad ka käesoleva määruse kohaselt kasutaja autentimiseks pakutavate Euroopa digiidentiteeditaskute kasutamist üksnes kasutaja vabatahtliku taotluse korral ja selliste miinimumandmete puhul, mis on vajalikud konkreetse internetipõhise teenuse kasutamiseks, mille jaoks autentimist nõutakse.

4. Komisjon soodustab ja hõlbustab koostöös liikmesriikidega tegevusjuhendite väljatöötamist, et aidata kaasa käesoleva määruse kohaldamisalasse kuuluvate Euroopa digiidentiteeditaskute laialdasele kättesaadavusele ja kasutatavusele. Tegevusjuhenditega lihtsustatakse e-identimise vahendite, sealhulgas käesoleva määruse kohaldamisalasse kuuluvate Euroopa digiidentiteeditaskute laialdast aktsepteerimist teenuseosutajate poolt, eelkõige nende teenuseosutajate poolt, kes kasutavad kasutajate autentimiseks kolmandate isikute e-identimise teenuseid. Komisjon hõlbustab selliste tegevusjuhendite väljatöötamist tihedas koostöös kõigi asjaomaste sidusrühmadega ning kutsub teenuseosutajaid üles viima tegevusjuhendite väljatöötamine lõpule 12 kuu jooksul alates käesoleva määruse vastuvõtmisest ja hakkama neid tõhusalt rakendama 18 kuu jooksul alates määruse vastuvõtmisest.

5. Komisjon hindab 24 kuu jooksul pärast Euroopa digiidentiteeditaskute kasutuselevõttu digiidentiteeditaskute nõudlust, kättesaadavust ja kasutatavust näitavatele tõendite põhjal seda, kas täiendavatele eraõiguslikele internetipõhiste teenuste osutajatele tuleks panna kohustus aktsepteerida kasutaja vabatahtliku taotluse korral Euroopa digiidentiteeditaskute kasutamist. Hindamiskriteeriumid hõlmavad kasutajabaasi ulatust, teenuseosutajate piiriülest tegutsemist, tehnoloogia arengut, kasutusviiside muutumist ja tarbijate nõudlust.“

8) Artikli 7 ette lisatakse järgmine pealkiri:

„II JAGU

E-IDENTIMISE SÜSTEEMID“.

9) Artikli 7 sissejuhatav lause asendatakse järgmisega:

„Vastavalt artikli 9 lõikele 1 teatavad liikmesriigid, kes ei ole seda veel teinud, 24 kuu jooksul pärast artikli 6a lõikes 11 ja artikli 6c lõikes 4 osutatud rakendusaktide jõustumist vähemalt ühest e-identimise süsteemist, mis sisaldab vähemalt üht identimisvahendit, mille usaldusväärsuse tase on kõrge. E-identimise süsteemist saab vastavalt artikli 9 lõikele 1 teavitada juhul, kui täidetud on kõik järgmised tingimused:“.

10) Artikli 9 lõiked 2 ja 3 asendatakse järgmisega:

„2. Komisjon avaldab *Euroopa Liidu Teatajas* nimekirja e-identimise süsteemidest, millest on teavitatud vastavalt käesoleva artikli lõikele 1, ja nendega seotud põhiteabe.

3. Komisjon avaldab lõikes 2 osutatud nimekirja muudatused *Euroopa Liidu Teatajas* ühe kuu jooksul pärast selle teate saamist.“

12) Lisatakse järgmine artikkel 11 a:

„*Artikkel 11a*

Andmete kokkulangevuse tagamine

1. Kui teavitatud e-identimise vahendeid või Euroopa digiidentiteeditaskuid kasutatakse autentimiseks, tagavad liikmesriigid tuginevate isikutena tegutsedes andmete kokkulangevuse tagamise.

2. Euroopa digiidentiteeditaskute pakkumisel lisavad liikmesriigid artikli 12 lõike 4 punktis d osutatud minimaalse hulga isikutuvastamisandmete hulka vähemalt ühe kordumatu ja püsiva identifikaatori kooskõlas liidu ja siseriikliku õigusega, et kasutaja tema taotluse korral identida, kui kasutaja identifitseerimine on seadusega nõutav.

2a. Liikmesriigid näevad ette tehnilised ja korralduslikud meetmed, et tagada andmete võrdlemiseks kasutatavate isikuandmete kõrgetasemeline kaitse ja vältida kasutajate profiilianalüüsi.

2aa. Liikmesriigid võivad kooskõlas siseriikliku õigusega ette näha, et Euroopa digiidentiteeditasku kasutajal on võimalik taotleda, et minimaalsete isikutuvastamisandmete hulka kuuluv ja artikli 6a lõike 4 punkti e kohaselt digiidentiteeditaskuga seotud kordumatu ja püsiv identifikaator asendatakse teise kordumatu ja püsiva identifikaatoriga, mille on välja andnud liikmesriik.

3. Kuue kuu jooksul pärast käesoleva määruse jõustumist täpsustab komisjon lõikes 1 osutatud meetmeid, võttes vastu rakendusakti. Kõnealune rakendusakt võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

3a Kuue kuu jooksul pärast käesoleva määruse jõustumist täpsustab komisjon lõigetes 2 ja 2aa osutatud meetmeid, võttes vastu rakendusakti. Kõnealune rakendusakt võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

13) Artiklit 12 muudetakse järgmiselt:

Koostöö ja koosvõime

a) lõike 3 punkt d jäetakse välja;

b) lõike 4 punkt d asendatakse järgmisega:

„d) viide minimaalsele hulgale isikutuvastamisandmetele, mida on vaja füüsilise isiku, juriidilise isiku või füüsilist või juriidilist isikut esindava füüsilise isiku kordumatuks ja püsivaks tähistamiseks;“

ba) lõikesse 5 lisatakse punkt c:

„c) sarnane lähenemisviis internetipõhistele teenustele, mille puhul aktsepteeritakse käesoleva määruse kohaselt pakutavate Euroopa digiidentiteeditaskute kasutamist;“

c) lõike 6 punkt a asendatakse järgmisega:

„a) teabe, kogemuste ja heade tavade vahetamine e-identimise süsteemide ning eelkõige koostalitlusvõime, andmete kokkulangevuse tagamise ja usaldusväärsuse tasemetega seotud tehniliste nõuete kohta;“

ca) lõikesse 6 lisatakse punkt e:

„e) teabe, kogemuste ja heade tavade vahetamine ning suuniste andmine selle kohta, kuidas kavandada, arendada ja rakendada internetipõhiseid teenuseid eesmärgiga tugineda Euroopa digiidentiteeditaskutele.“

14) Lisatakse artiklid 12a ja 12b:

„*Artikkel 12a*

E-identimise süsteemide sertifitseerimine

1. Selliste e-identimise süsteemide, millest tuleb teavitada, vastavust käesolevas määruses sätestatud nõuetele sertifitseeritakse, et tõendada selliste süsteemide või nende osade vastavust artikli 8 lõikes 2 sätestatud nõuetele seoses sellega, mis puudutab e-identimise kavade usaldusväärsuse tasemeid vastavalt määruse (EL) 2019/881 kohasele asjaomasele küberturvalisuse sertifitseerimise kavale või selle osadele, kui küberturvalisuse sertifikaat või selle osad hõlmavad artikli 8 lõikes 2 sätestatud nõudeid e-identimise süsteemide usaldusväärsuse tasemete kohta. Sertifitseerimine kehtib kuni viis aastat, sõltuvalt korrapärasest nõrkuste hindamisest iga kahe aasta tagant. Kui tehakse kindlaks nõrkused ja neid ei kõrvaldata kolme kuu jooksul, sertifitseerimine tühistatakse.

   Sertifitseerimist teostavad liikmesriikide määratud akrediteeritud avalik-õiguslikud või eraõiguslikud vastavushindamisasutused kooskõlas määrusega (EÜ) nr 765/2008.

2. Artikli 12 lõike 6 punktis c osutatud e-identimise süsteemide vastastikust hindamist ei kohaldata lõike 1 kohaselt sertifitseeritud e-identimise süsteemide või nende osade suhtes.

2a. Olenemata käesoleva artikli lõikest 2 võivad liikmesriigid nõuda teavitavalt liikmesriigilt lisateavet käesoleva artikli lõike 2 kohaselt sertifitseeritud e-identimise süsteemide või nende osade kohta.

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

Artikkel 12b

Juurdepääs riist- ja tarkvarafunktsioonidele

Euroopa digiidentiteeditaskute väljastajad ja teavitatud e-identimise vahendite väljastajad, kes tegutsevad äri- või kutsetegevuse raames ja kasutavad määruse (EL) 2022/1925 artikli 2 lõikes 2 määratletud põhiplatvormiteenuseid lõppkasutajatele Euroopa digiidentiteeditasku teenuste ja e-identimise vahendite pakkumiseks või selle käigus, on ärikasutajad vastavalt määruse (EL) 2022/1925 artikli 2 punktile 21.“

17) Artikli 13 lõige 1 asendatakse järgmisega:

„1. Olenemata käesoleva artikli lõikest 2, 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.“

18) Artikkel 14 asendatakse järgmisega:

„*Artikkel 14*

Rahvusvahelised aspektid

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

2. Lõikes 1 osutatud rakendusotsuste ja kokkulepetega tagatakse, et kolmanda riigi usaldusteenuse osutajad või rahvusvahelised organisatsioonid ning nende osutatavad teenused vastavad liidus asuvate kvalifitseeritud usaldusteenuse osutajate ja nende osutatavate kvalifitseeritud usaldusteenuste suhtes kohaldatavatele nõuetele. Eelkõige koostavad, haldavad ja avaldavad kolmandad riigid ja rahvusvahelised organisatsioonid tunnustatud usaldusteenuse osutajate usaldusnimekirja.

   Lõikes 1 osutatud kokkulepetega tagatakse, et 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.

3. Lõikes 1 osutatud rakendusotsused võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

19) Artikkel 15 asendatakse järgmisega:

„*Artikkel 15*

Kättesaadavus puuetega inimeste jaoks

Usaldusteenuste osutamine ja nende teenuste osutamisel kasutatavad lõppkasutajale suunatud tooted tehakse puuetega inimestele kättesaadavaks kooskõlas ligipääsetavusnõuetega, mis on sätestatud direktiivis (EL) 2019/882 toodete ja teenuste ligipääsetavusnõuete kohta.“

20) Artiklit 17 muudetakse järgmiselt:

a) lõiget 4 muudetakse järgmiselt:

1) lõike 4 punkt c asendatakse järgmisega:

„c) teavitada asjaomaste liikmesriikide asjaomaseid pädevaid asutusi, mis on määratud direktiivi (EL) XXXX/XXXX [NIS2 direktiiv] kohaselt, kõigist olulistest turvarikkumistest või tervikluse kaost, millest nad oma ülesannete täitmisel teada saavad. Kui oluline turvarikkumine või tervikluse kadu puudutab teisi liikmesriike, teavitab järelevalveasutus sellest direktiivi (EL) XXXX/XXXX [NIS2 direktiiv] kohaselt määratud asjaomase liikmesriigi ühtset kontaktpunkti ja käesoleva määruse artikli 17 kohaselt määratud järelevalveasutusi teistes asjaomastes liikmesriikides. Kui teavitatud järelevalveasutus leiab, et turvarikkumise või tervikluse kao avalikustamine on avalikes huvides, teavitab ta üldsust või nõuab üldsuse teavitamist asjaomaselt usaldusteenuse osutajalt;“

2) punkt f asendatakse järgmisega:

„f) teha koostööd määruse (EL) 2016/679 alusel loodud pädevate järelevalveasutustega, eelkõige teavitades neid põhjendamatu viivituseta sellest, kui isikuandmete kaitse eeskirju on ilmselt rikutud, ja turvarikkumistest, mis kujutavad endast ilmselt isikuandmetega seotud rikkumisi;“

b) lõige 6 asendatakse järgmisega:

„6. Iga aasta 31. märtsiks esitab iga järelevalveasutus komisjonile aruande oma põhitegevuse kohta eelmisel kalendriaastal.“;

c) lõige 8 asendatakse järgmisega:

„8. 12 kuu jooksul alates käesoleva määruse jõustumisest võtab komisjon vastu suunised järelevalveasutuste lõikes 4 osutatud ülesannete täitmise kohta ning määrab artikli 48 lõikes 2 osutatud kontrollimenetluse kohaselt vastu võetud rakendusaktidega kindlaks lõikes 6 osutatud aruande formaadid ja menetlused.“

21) Artiklit 18 muudetakse järgmiselt:

a) artikli 18 pealkiri asendatakse järgmisega:

„Vastastikune abi ja koostöö“;

b) lõige 1 asendatakse järgmisega:

„1. Järelevalveasutused teevad koostööd, et vahetada häid tavasid ja teavet usaldusteenuste osutamise kohta.“;

c) lisatakse lõiked 4 ja 5:

„4. Järelevalveasutused ja Euroopa Parlamendi ja nõukogu direktiivi (EL) XXXX/XXXX [NIS2 direktiiv] kohased riiklikud pädevad asutused teevad koostööd ja abistavad üksteist, et tagada usaldusteenuse osutajate vastavus käesoleva määruse ja direktiivi (EL) XXXX/XXXX [NIS2 direktiiv] nõuetele. Järelevalveasutused paluvad direktiivi XXXX/XXXX [NIS2 direktiiv] kohastel riiklikel pädevatel asutustel võtta järelevalvemeetmeid, et kontrollida usaldusteenuse osutajate vastavust direktiivi XXXX/XXXX (NIS2 direktiiv) nõuetele, nõuda usaldusteenuse osutajatelt nende nõuete rikkumise heastamist, esitada õigeaegselt usaldusteenuse osutajatega seotud mis tahes järelevalvetegevuse tulemused ning teavitada järelevalveasutusi direktiivi XXXX/XXXX [NIS2 direktiiv] kohaselt teatatud intsidentidest.

5. 12 kuu jooksul pärast käesoleva määruse jõustumist kehtestab komisjon rakendusaktidega vajaliku menetluskorra lõikes 1 osutatud järelevalveasutustevahelise koostöö hõlbustamiseks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

21a) Lisatakse järgmine artikkel 19a:

„Nõuded kvalifitseerimata usaldusteenuse osutajatele

1. Kvalifitseerimata usaldusteenuseid osutav kvalifitseerimata usaldusteenuse osutaja:

a) omab asjakohaseid tegevuspõhimõtteid ja võtab vastavaid meetmeid, et juhtida kvalifitseerimata usaldusteenuse osutamisega seotud õiguslikke, ärilisi, tegevuslikke ja muid otseseid või kaudseid riske. Olenemata direktiivi EL XXXX/XXX [NIS2 direktiiv] artikli 18 sätetest hõlmavad need meetmed vähemalt järgmist:

i) meetmed, mis on seotud teenuse kasutamiseks registreerimise ja kliendisuhete loomisega;

ii) meetmed, mis on seotud menetlus- või halduskontrolliga;

iii) meetmed, mis on seotud teenuste haldamise ja rakendamisega;

b) teavitab järelevalveasutust, tuvastatavaid mõjutatud isikuid, avalikkust, kui see on avalikes huvides, ja vajaduse korral teisi asjaomaseid pädevaid asutusi teenuse osutamisel esinenud kõigist rikkumistest või häiretest või lõike a punktides i, ii ja iii osutatud meetmete rakendamisest, millel on märkimisväärne mõju osutatavale usaldusteenusele või seal säilitatavatele isikuandmetele, tehes seda põhjendamatu viivituseta ja igal juhul hiljemalt 24 tunni jooksul pärast sellest teadasaamist.

2. 12 kuu jooksul pärast käesoleva määruse jõustumist täpsustab komisjon rakendusaktidega lõike 1 punktis a osutatud meetmete tehnilised omadused. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

22) Artiklit 20 muudetakse järgmiselt:

a) lõige 1 asendatakse järgmisega:

„1. Vastavushindamisasutus auditeerib kvalifitseeritud usaldusteenuse osutajaid nende oma kulul vähemalt iga 24 kuu järel. Auditiga kinnitatakse, et kvalifitseeritud usaldusteenuse osutajad ja nende osutatavad kvalifitseeritud usaldusteenused vastavad käesolevas määruses ja direktiivi (EL) XXXX/XXXX [NIS2 direktiiv] artiklis 18 sätestatud nõuetele. Kvalifitseeritud usaldusteenuse osutajad esitavad saadud vastavushindamisaruande järelevalveasutusele kolme tööpäeva jooksul alates selle kättesaamisest.“;

aa) lisatakse järgmine lõige:

1a. Liikmesriigid võivad ette näha, et kvalifitseeritud usaldusteenuse osutajad teavitavad järelevalveasutust eelnevalt kavandatavatest audititest ja võimaldavad järelevalveasutusel taotluse korral vaatlejana osaleda.“;

b) punkti 2 viimane lause asendatakse järgmisega:

„Kui isikuandmete kaitse eeskirju on ilmselt rikutud, teavitab järelevalveasutus põhjendamatu viivituseta määruse (EL) 2016/679 kohaseid pädevaid järelevalveasutusi.“;

c) lõiked 3 ja 4 asendatakse järgmisega:

„3. Kui kvalifitseeritud usaldusteenuse osutaja ei täida mõnda käesolevas määruses sätestatud nõuet, nõuab järelevalveasutus, et ta tagaks vajaduse korral kindlaksmääratud tähtaja jooksul heastamise.

Kui teenuseosutaja ei taga heastamist, asjakohasel juhul järelevalveasutuse kehtestatud tähtaja jooksul, võib järelevalveasutus, võttes eelkõige arvesse kõnealuse rikkumise ulatust, kestust ja tagajärgi, sellelt teenuseosutajalt või tema osutatavalt mõjutatud teenuselt kvalifitseeritud staatuse ära võtta.

3a. Kui riiklikud pädevad asutused teatavad direktiivi (EL) XXXX/XXXX [NIS2 direktiiv] kohaselt järelevalveasutusele, et kvalifitseeritud usaldusteenuse osutaja ei täida mõnda direktiivi (EL) XXXX/XXXX [NIS2] artiklis 18 sätestatud nõuet, võib järelevalveasutus, võttes eelkõige arvesse rikkumise ulatust, kestust ja tagajärgi, sellelt teenuseosutajalt või tema osutatavalt mõjutatud teenuselt kvalifitseeritud staatuse ära võtta.

3b. Kui järelevalveasutused teatavad määruse (EL) 2016/679 kohaselt järelevalveasutusele, et kvalifitseeritud usaldusteenuse osutaja ei täida mõnda määruses (EL) 2016/679 sätestatud nõuet, võib järelevalveasutus, võttes eelkõige arvesse rikkumise ulatust, kestust ja tagajärgi, kõnealuselt teenuseosutajalt või tema osutatavalt teenuselt kvalifitseeritud staatuse ära võtta.

3c. Järelevalveasutus teavitab kvalifitseeritud usaldusteenuse osutajat temalt kvalifitseeritud staatuse või asjaomaselt teenuselt kvalifitseeritud staatuse äravõtmisest. Järelevalveasutus teavitab artikli 22 lõikes 3 osutatud asutust, eesmärgiga ajakohastada artikli 22 lõikes 1 osutatud usaldusnimekirju, ning teavitab direktiivis (EL) XXXX/XXXX [NIS2 direktiiv] osutatud riiklikku pädevat asutust.

4. Komisjon kehtestab rakendusaktidega 12 kuu jooksul pärast käesoleva määruse jõustumist tehnilised kirjeldused ja standardite viitenumbrid järgmistel eesmärkidel:

a) vastavushindamisasutuste akrediteerimine ja lõikes 1 osutatud vastavushindamisaruanne;

b) auditeerimisnõuded, mille alusel vastavushindamisasutused hindavad kvalifitseeritud usaldusteenuse osutajate nõuetele vastavust, nagu on osutatud lõikes 1;

c) vastavushindamissüsteemid kvalifitseeritud usaldusteenuse osutajate vastavushindamiseks vastavushindamisasutuste poolt ja lõikes 1 osutatud aruande esitamiseks.

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

23) Artiklit 21 muudetakse järgmiselt:

„1. Kui usaldusteenuse osutajad kavatsevad alustada kvalifitseeritud usaldusteenuse osutamist, esitavad nad järelevalveasutusele oma kavatsuse kohta teate koos vastavushindamisasutuse väljastatud vastavushindamisaruandega, milles kinnitatakse käesolevas määruses ja direktiivi (EL) XXXX/XXXX [NIS2 direktiiv] artiklis 18 sätestatud nõuete täitmist.“;

a) lõige 2 asendatakse järgmisega:

„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.

Et kontrollida usaldusteenuse osutaja vastavust direktiivi XXXX [NIS2 direktiiv] artikli 18 nõuetele, nõuab järelevalveasutus, et direktiivis XXXX [NIS2 direktiiv] osutatud pädevad asutused võtaksid sellega seoses järelevalvemeetmeid ja esitaksid tulemuste kohta teabe põhjendamatu viivituseta ja hiljemalt kahe kuu jooksul pärast seda, kui direktiivis XXXX [NIS2 direktiiv] osutatud pädevad asutused on selle taotluse kätte saanud. Kui kontrolli ei ole kahe kuu jooksul alates teavitamisest lõpule viidud, teavitavad direktiivis XXXX [NIS2 direktiiv] osutatud pädevad asutused järelevalveasutust viivituse põhjustest ja ajavahemikust, mille jooksul kontroll lõpule viiakse.

Kui järelevalveasutus leiab, et usaldusteenuse osutaja ja tema osutatavad teenused vastavad käesolevas määruses sätestatud 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.“;

b) lõige 4 asendatakse järgmisega:

„4. 12 kuu jooksul pärast käesoleva määruse jõustumist määrab komisjon rakendusaktidega kindlaks teavitamise ja kontrollimise formaadid ja menetlused lõigete 1 ja 2 kohaldamiseks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

25) Artiklit 24 muudetakse järgmiselt:

a) lõige 1 asendatakse järgmisega:

„1. Kvalifitseeritud sertifikaati või kvalifitseeritud elektroonilist atribuutide tõendit väljastades kontrollib kvalifitseeritud usaldusteenuse osutaja selle füüsilise või juriidilise isiku identiteeti ja vajaduse korral konkreetseid atribuute, kellele kvalifitseeritud sertifikaat või kvalifitseeritud elektrooniline atribuutide tõend väljastatakse.

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

a) kasutades Euroopa digiidentiteeditaskut või teavitatud e-identimise vahendit, mis vastab artiklis 8 sätestatud nõuetele seoses kõrge usaldusväärsuse tasemega;

b) kooskõlas punktiga a, c või d väljastatud kvalifitseeritud elektroonilise atribuutide tõendi või kvalifitseeritud e-allkirja sertifikaadi või kvalifitseeritud e-templi sertifikaadi abil;

c) kasutades muid identifitseerimismeetodeid, mis tagavad isiku kõrgetasemelise usaldusväärsusega tuvastamise, mille vastavust kinnitab vastavushindamisasutus;

d) füüsilise isiku või juriidilise isiku volitatud esindaja füüsilise kohaloleku alusel asjakohaste menetluste kohaselt ja kooskõlas siseriiklike õigusaktidega.“;

b) lisatakse järgmine lõige 1 a:

„1a. „12 kuu jooksul pärast käesoleva määruse jõustumist kehtestab komisjon rakendusaktidega minimaalsed tehnilised kirjeldused, standardid ja menetlused seoses identiteedi ja atribuutide kontrollimisega vastavalt lõike 1 punktile c. Kõnealused rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“;

c) lõiget 2 muudetakse järgmiselt:

0) punkti a muudetakse järgmiselt:

„a) teavitab järelevalveasutust vähemalt üks kuu enne mis tahes muudatuse rakendamist kvalifitseeritud usaldusteenuse osutamisel või vähemalt kolm kuud enne, juhul kui on kavatsus selline tegevus lõpetada. Järelevalveasutus võib enne kvalifitseeritud usaldusteenustes kavandatud muudatuste tegemiseks loa andmist nõuda lisateavet või vastavushindamise tulemusi. Kui kontrolli ei ole kolme kuu jooksul alates teavitamisest lõpule viidud, teavitab järelevalveasutus usaldusteenuse osutajat viivituse põhjustest ja ajavahemikust, mille jooksul kontroll lõpule viiakse.

1) punktid d ja e asendatakse järgmisega:

„d) teavitab enne lepingu sõlmimist kõiki kvalifitseeritud usaldusteenust kasutada soovivaid isikuid selgelt, põhjalikult ja hõlpsasti juurdepääsetaval viisil, avalikult juurdepääsetavas ruumis ja isiklikult kõnealuse teenuse kasutamise täpsetest tingimustest, sealhulgas kõigist selle kasutamise piirangutest;“

„e) kasutab muutmise eest kaitstud usaldusväärseid süsteeme ja tooteid ning tagab nende toetatavate protsesside tehnilise turvalisuse ja usaldusväärsuse, sealhulgas kasutab sobivaid krüptograafilisi algoritme, võtmepikkusi ja räsifunktsioone süsteemides, toodetes ja nendega toetatavates protsessides;“

2) lisatakse punktid fa ja fb:

„fa) omab asjakohaseid tegevuspõhimõtteid ja võtab vastavaid meetmeid, et juhtida kvalifitseeritud usaldusteenuse osutamisega seotud õiguslikke, ärilisi, tegevuslikke ja muid otseseid või kaudseid riske. Olenemata direktiivi EL XXXX/XXX [NIS2 direktiiv] artikli 18 sätetest hõlmavad need meetmed vähemalt järgmist:

i) meetmed, mis on seotud teenuse kasutamiseks registreerimise ja kliendisuhete loomisega;

ii) meetmed, mis on seotud menetlus- või halduskontrolliga;

iii) meetmed, mis on seotud teenuste haldamise ja rakendamisega;

„fb) teavitab järelevalveasutust, tuvastatavaid mõjutatud isikuid, kohaldataval juhul teisi asjaomaseid pädevaid asutusi ning järelevalveasutuse taotlusel ka avalikkust, kui see on avalikes huvides, teenuse osutamisel esinenud kõigist rikkumistest või häiretest või punkti fa alapunktides i, ii ja iii osutatud meetmete rakendamisest, millel on märkimisväärse mõju osutatavale usaldusteenusele või seal säilitatavatele isikuandmetele, tehes seda põhjendamatu viivituseta ja igal juhul hiljemalt 24 tunni jooksul pärast intsidenti;“

3) punktid g ja h asendatakse järgmisega:

„g) võtab asjakohaseid meetmeid andmete võltsimise, varguse või omastamise vastu või andmete loata kustutamise, muutmise või ligipääsmatuks muutmise vastu;

„h) salvestab kogu asjakohase teabe kvalifitseeritud usaldusteenuse osutaja väljastatud ja saadud andmete kohta ja hoiab seda kättesaadavana nii kaua kui vajalik pärast seda, kui kvalifitseeritud usaldusteenuse osutaja on tegevuse lõpetanud, et esitada tõendeid kohtumenetlustes ja tagada teenuse järjepidevus. Need andmed võib salvestada elektrooniliselt;“

4) punkt j jäetakse välja;

d) lisatakse järgmine lõige 4a:

„4a. Kvalifitseeritud elektrooniliste atribuutide tõendite kehtetuks tunnistamise suhtes kohaldatakse vastavalt lõikeid 3 ja 4.“;

e) lõige 5 asendatakse järgmisega:

„5. 12 kuu jooksul pärast käesoleva määruse jõustumist kehtestab komisjon rakendusaktidega tehnilised kirjeldused, menetlused ja standardite viitenumbrid lõikes 2 osutatud nõuete jaoks. Kui neid tehnilisi kirjeldusi, menetlusi ja standardeid järgitakse, loetakse käesolevas artiklis sätestatud nõuded täidetuks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“;

f) lisatakse järgmine lõige 6:

„6. Komisjonil on õigus võtta vastu rakendusakte, milles täpsustatakse lõike 2 punktis fa osutatud meetmete tehnilised omadused.“

25a) Artiklit 26 muudetakse järgmiselt:

2. 12 kuu jooksul pärast käesoleva määruse jõustumist kehtestab komisjon rakendusaktidega täiustatud e-allkirjade tehnilised kirjeldused ja asjakohaste standardite viitenumbrid. Kui täiustatud e-allkiri vastab kõnealustele tehnilistele kirjeldustele ja standarditele, loetakse täiustatud e-allkirjadele esitatavad nõuded täidetuks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

25b) Artiklit 27 muudetakse järgmiselt:

lõige 4 jäetakse välja.

26) Artikli 28 lõige 6 asendatakse järgmisega:

„6. 12 kuu jooksul pärast käesoleva määruse jõustumist kehtestab komisjon rakendusaktidega e-allkirjade kvalifitseeritud sertifikaatide tehnilised kirjeldused ja asjakohaste standardite viitenumbrid. Kui e-allkirja kvalifitseeritud sertifikaat vastab kõnealustele tehnilistele kirjeldustele ja standarditele, loetakse I lisas sätestatud nõuded täidetuks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

27) Artiklisse 29 lisatakse järgmine lõige 1a:

„1a. E-allkirja andmiseks vajalikke andmeid võib allkirja andja nimel luua, hallata või varundamise eesmärgil dubleerida üksnes kvalifitseeritud usaldusteenuse osutaja, kes osutab kvalifitseeritud usaldusteenust kvalifitseeritud e-allkirja vahemaa tagant andmise vahendi haldamiseks.“

28) Lisatakse järgmine artikkel 29a:

„*Artikkel 29a*

Nõuded kvalifitseeritud e-allkirja vahemaa tagant andmise vahendi haldamise kvalifitseeritud teenusele

1. Kvalifitseeritud e-allkirja vahemaa tagant andmise vahendit võib kvalifitseeritud teenusena hallata üksnes kvalifitseeritud usaldusteenuse osutaja, kes:

   a) loob allkirja andja nimel e-allkirja andmiseks vajalikke andmeid või haldab neid;

   b) olenemata II lisa punkti 1 alapunktist d võib dubleerida e-allkirja andmiseks vajalikke andmeid ainult varundamise eesmärgil, kui on täidetud järgmised nõuded:

      i. dubleeritud andmekogumi turvatase peab olema sama mis algsel andmekogumil;

      ii. dubleeritud andmekogumite arv ei ületa teenuse järjepidevuse tagamiseks vajalikku miinimumi;

   c) vastab kõigile nõuetele, mis on kindlaks määratud artikli 30 kohaselt väljastatud konkreetse kvalifitseeritud e-allkirja vahemaa tagant andmise vahendi sertifitseerimisaruandes.

2. Komisjon kehtestab rakendusaktidega 12 kuu jooksul pärast käesoleva määruse jõustumist tehnilised kirjeldused ja standardite viitenumbrid lõike 1 kohaldamiseks.“

29) Artiklisse 30 lisatakse lõige 3a järgmises sõnastuses:

„3a. Lõikes 1 osutatud sertifitseerimine kehtib kuni viis aastat ja sõltub korrapärasest nõrkuste hindamisest iga kahe aasta tagant. Kui tehakse kindlaks nõrkused ja neid ei kõrvaldata, sertifitseerimine tühistatakse.“

30) Artikli 31 lõige 3 asendatakse järgmisega:

„3. Komisjon kehtestab rakendusaktidega 12 kuu jooksul pärast käesoleva määruse jõustumist lõike 1 kohaldamisega seotud formaadid ja menetlused. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

31) Artiklit 32 muudetakse järgmiselt:

a) lõikesse 1 lisatakse järgmine lõik:

„Kui kvalifitseeritud e-allkirjade valideerimine vastab lõikes 3 osutatud kirjeldustele ja standarditele, loetakse esimeses lõigus sätestatud nõuded täidetuks.“;

b) lõige 3 asendatakse järgmisega:

„3. 12 kuu jooksul pärast käesoleva määruse jõustumist kehtestab komisjon rakendusaktidega kvalifitseeritud e-allkirjade valideerimise kirjeldused ja standardite viitenumbrid. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

31a) Lisatakse järgmine artikkel 32a:

„Kvalifitseeritud sertifikaatidel põhinevate täiustatud e-allkirjade valideerimise nõuded

1. Kvalifitseeritud sertifikaadil põhineva täiustatud e-allkirja valideerimise protsess kinnitab kvalifitseeritud sertifikaadil põhineva täiustatud 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) allkirjastatud andmete terviklust ei ole rikutud;

g) artiklis 26 sätestatud nõuded olid allkirja andmise ajal täidetud. Kui kvalifitseeritud sertifikaadil põhineva täiustatud e-allkirja valideerimine vastab lõikes 3 osutatud kirjeldustele ja standarditele, loetakse esimeses lõigus sätestatud nõuded täidetuks.

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

3. 12 kuu jooksul pärast käesoleva määruse jõustumist kehtestab komisjon rakendusaktidega kvalifitseeritud sertifikaatidel põhinevate täiustatud e-allkirjade valideerimise kirjeldused ja standardite viitenumbrid. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

31b) Artiklit 33 muudetakse järgmiselt:

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

„2. 12 kuu jooksul pärast käesoleva määruse jõustumist kehtestab komisjon rakendusaktidega lõikes 1 osutatud kvalifitseeritud valideerimisteenuse tehnilised kirjeldused ja standardite viitenumbrid. Kui kvalifitseeritud e-allkirjade valideerimisteenus vastab kõnealustele kirjeldustele ja standarditele, loetakse lõikes 1 sätestatud nõuded täidetuks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

32) Artikkel 34 asendatakse järgmisega:

„*Artikkel 34*

Kvalifitseeritud e-allkirjade kvalifitseeritud säilitamisteenus

1. Kvalifitseeritud e-allkirjade kvalifitseeritud säilitamisteenust 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. Kui kvalifitseeritud e-allkirjade kvalifitseeritud säilitamisteenuse suhtes kohaldatav kord vastab lõikes 3 osutatud kirjeldustele ja standarditele, loetakse lõikes 1 sätestatud nõuded täidetuks.

3. 12 kuu jooksul pärast käesoleva määruse jõustumist kehtestab komisjon rakendusaktidega kvalifitseeritud e-allkirjade kvalifitseeritud säilitamisteenuse tehnilised kirjeldused ja standardite viitenumbrid. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

32a) Artiklisse 36 lisatakse uus lõige 2:

2. 12 kuu jooksul pärast käesoleva määruse jõustumist kehtestab komisjon rakendusaktidega täiustatud e-templite tehnilised kirjeldused ja asjakohaste standardite viitenumbrid.

Kui täiustatud e-tempel vastab kõnealustele tehnilistele kirjeldustele ja standarditele, loetakse täiustatud e-templitele esitatavad nõuded täidetuks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

33) Artiklit 37 muudetakse järgmiselt:

lõige 4 jäetakse välja.

34) Artiklit 38 muudetakse järgmiselt:

a) lõige 1 asendatakse järgmisega:

„1. E-templi kvalifitseeritud sertifikaadid peavad vastama III lisas sätestatud nõuetele. Kui e-templi kvalifitseeritud sertifikaat vastab lõikes 6 osutatud kirjeldustele ja standarditele, loetakse III lisas sätestatud nõuded täidetuks.“;

b) lõige 6 asendatakse järgmisega:

„6. 12 kuu jooksul pärast käesoleva määruse jõustumist kehtestab komisjon rakendusaktidega e-templite kvalifitseeritud sertifikaatide tehnilised kirjeldused ja asjakohaste standardite viitenumbrid. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

35) Lisatakse järgmine artikkel 39a:

„*Artikkel 39a*

Nõuded kvalifitseeritud e-templi vahemaa tagant loomise vahendi haldamise kvalifitseeritud teenusele

Artiklit 29a kohaldatakse *mutatis mutandis* kvalifitseeritud e-templi vahemaa tagant loomise vahendi haldamise kvalifitseeritud teenuse suhtes.“

35a) Lisatakse järgmine artikkel 40a:

„*Artikkel 40a*

Kvalifitseeritud sertifikaatidel põhinevate täiustatud e-templite valideerimise nõuded

1) Kvalifitseeritud sertifikaatidel põhinevate täiustatud e-templite valideerimise suhtes kohaldatakse *mutatis mutandis* artiklit 32a.“

36) Artiklit 42 muudetakse järgmiselt:

a) lisatakse uus lõige 1a:

„1a. Kui kuupäeva ja ajahetke andmetega sidumine ja täpne ajaallikas vastavad lõikes 2 osutatud kirjeldustele ja standarditele, loetakse lõikes 1 sätestatud nõuded täidetuks.“;

b) lõige 2 asendatakse järgmisega:

„2. 12 kuu jooksul pärast käesoleva määruse jõustumist kehtestab komisjon rakendusaktidega kuupäeva ja ajahetke andmetega sidumise ja täpse ajaallika tehnilised kirjeldused ja standardite viitenumbrid. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

36a) Artiklisse 43 lisatakse lõige 3:

2a. Ühe liikmesriigi kvalifitseeritud registreeritud e-andmevahetusteenust tunnustatakse kvalifitseeritud registreeritud e-andmevahetusteenusena kõikides liikmesriikides.“

37) Artiklit 44 muudetakse järgmiselt:

a) lisatakse järgmine lõige 1a:

„1a. Kui andmete saatmise ja kättesaamise protsess vastab lõikes 2 osutatud kirjeldustele ja standarditele, loetakse lõikes 1 sätestatud nõuded täidetuks.“;

b) lõige 2 asendatakse järgmisega:

„2. 12 kuu jooksul pärast käesoleva määruse jõustumist kehtestab komisjon rakendusaktidega andmete saatmise ja kättesaamise protsessi tehnilised kirjeldused ja standardite viitenumbrid. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“;

c) lisatakse lõiked 3 ja 4:

„3. Kvalifitseeritud registreeritud e-andmevahetusteenuste osutajad võivad kokku leppida nende osutatavate kvalifitseeritud registreeritud e-andmevahetusteenuste koostalitlusvõimes. Selline koostalitlusvõime raamistik peab vastama lõikes 1 sätestatud nõuetele. Nõuete täitmine peab olema vastavushindamisasutuse poolt kinnitatud.

„4. Komisjon võib rakendusaktiga kehtestada tehnilised kirjeldused ja standardite viitenumbrid, et hõlbustada andmete edastamist kahe või enama kvalifitseeritud usaldusteenuse osutaja vahel. Tehnilised kirjeldused ja standardite sisu peavad olema kulutõhusad ja proportsionaalsed. Rakendusakt võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

38) Artikkel 45 asendatakse järgmisega:

„*Artikkel 45*

Nõuded veebisaidi autentimise kvalifitseeritud sertifikaatidele

1. Veebisaidi autentimise kvalifitseeritud sertifikaadid peavad vastama IV lisas sätestatud nõuetele. IV lisas sätestatud nõuetele vastavust hinnatakse vastavalt lõikes 4 osutatud kirjeldustele ja standarditele.

2. Veebibrauserid tunnustavad lõikes 1 osutatud veebisaidi autentimise kvalifitseeritud sertifikaate. Selleks tagavad veebibrauserite käitajad, et mis tahes meetodi abil esitatud identiteediandmed kuvatakse kasutajasõbralikul viisil. Veebibrauserid tagavad toetuse ja koostalitlusvõime lõikes 1 osutatud veebisaidi autentimise kvalifitseeritud sertifikaatidega, välja arvatud komisjoni soovituse 2003/361/EÜ kohaselt mikro- ja väikeettevõtjateks peetavate ettevõtjate puhul esimese viie aasta jooksul, mil nad tegutsevad veebilehitsemisteenuste pakkujatena.

4. 12 kuu jooksul pärast käesoleva määruse jõustumist kehtestab komisjon rakendusaktidega tehnilised kirjeldused ja standardite viitenumbrid lõigetes 1 ja 2 osutatud veebisaidi autentimise kvalifitseeritud sertifikaatide jaoks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

39) Artikli 45 järele lisatakse 9., 10. ja 11. jagu:

9. JAGU

ATRIBUUTIDE ELEKTROONILINE TÕENDAMINE

Artikkel 45a

Atribuutide elektroonilise tõendamise õiguslik toime

1. Atribuutide elektroonilist tõendit ei tunnistata õiguslikult kehtetuks ega kohtumenetlustes tõenduskõlbmatuks ainuüksi seetõttu, et see on elektroonilisel kujul või ei vasta kvalifitseeritud elektroonilistele atribuutide tõenditele esitatavatele nõuetele.

2. Kvalifitseeritud elektroonilisel atribuutide tõendil ja atribuutide tõenditel, mis on välja antud autentse allika eest vastutava avaliku sektori asutuse poolt või nimel, on samasugune õiguslik toime nagu seaduslikult väljastatud paberkandjal tõenditel.

3. Ühes liikmesriigis väljastatud kvalifitseeritud elektroonilist atribuutide tõendit tunnustatakse kvalifitseeritud elektroonilise atribuutide tõendina kõikides liikmesriikides.

4. Atribuutide tõendit, mis on väljastatud autentse allika eest vastutava avaliku sektori asutuse poolt või nimel, tunnustatakse atribuutide tõendina, mis on väljastatud autentse allika eest vastutava avaliku sektori asutuse poolt või nimel, kõigis liikmesriikides.

Artikkel 45b

Atribuutide elektrooniline tõendamine avalike teenuste puhul

Kui vastavalt siseriiklikule õigusele nõutakse avaliku sektori asutuse osutatavale internetipõhisele teenusele juurdepääsuks e-identimist e-identimise vahendi abil ja e-autentimist, ei asenda atribuutide elektroonilises tõendis sisalduvad isiku identimisandmed e-identimist e-identimise vahendi abil ja autentimist e-identimise eesmärgil, välja arvatud juhul, kui liikmesriik seda konkreetselt lubab. Sellisel juhul aktsepteeritakse ka teiste liikmesriikide kvalifitseeritud elektroonilisi atribuutide tõendeid.

Artikkel 45c

Kvalifitseeritud elektroonilistele atribuutide tõenditele esitatavad nõuded

1. Kvalifitseeritud elektrooniline atribuutide tõend peab vastama V lisas sätestatud nõuetele.

1a. V lisas sätestatud nõuetele vastavust hinnatakse vastavalt lõikes 4 osutatud kirjeldustele ja standarditele.

2. Kvalifitseeritud elektroonilise atribuutide tõendi suhtes ei kohaldata ühtegi kohustuslikku nõuet lisaks V lisas sätestatud nõuetele.

3. Kui kvalifitseeritud elektrooniline atribuutide tõend tühistatakse pärast esialgset väljastamist, kaotab see alates tühistamise hetkest kehtivuse ega saa oma staatust mingil juhul tagasi.

4. Kuue kuu jooksul pärast käesoleva määruse jõustumist kehtestab komisjon kvalifitseeritud elektrooniliste atribuutide tõendite tehnilised kirjeldused ja asjakohaste standardite viitenumbrid, võttes vastu artikli 6a lõikes 11 osutatud rakendusakti Euroopa digiidentiteeditaskute rakendamise kohta.

Artikkel 45d

Atribuutide kontrollimine autentsete allikate alusel

1. Liikmesriigid tagavad 24 kuu jooksul pärast artikli 6a lõikes 11 ja artikli 6c lõikes 4 osutatud rakendusaktide jõustumist, et vähemalt VI lisas loetletud atribuutide puhul, kui need atribuudid põhinevad avaliku sektori autentsetel allikatel, võetakse meetmed, mis võimaldavad atribuutide elektrooniliste tõendite kvalifitseeritud pakkujatel neid atribuute kasutaja taotlusel ja kooskõlas siseriikliku või liidu õigusega elektrooniliselt kontrollida.

2. Kuue kuu jooksul pärast käesoleva määruse jõustumist määrab komisjon asjakohaseid rahvusvahelisi standardeid arvesse võttes kindlaks minimaalsed tehnilised kirjeldused, standardid ja menetlused seoses atribuutide kataloogi ja tõendamise kavadega ning kontrollimenetlustega atribuutide kvalifitseeritud elektrooniliseks tõendamiseks, võttes vastu artikli 6a lõikes 11 osutatud rakendusakti Euroopa digiidentiteeditaskute rakendamise kohta.

Artikkel 45da

Autentse allika eest vastutava avaliku sektori asutuse poolt või nimel välja antud elektroonilistele atribuutide tõenditele esitatavad nõuded

1. Autentse allika eest vastutava avaliku sektori asutuse poolt või nimel välja antud elektrooniline atribuutide tõend peab vastama järgmistele nõuetele:

a) nõuded, mis on sätestatud VII lisas;

b) VII lisa punktis b osutatud väljaandjaks tunnistatud ja artikli 3 punktis 45a osutatud avaliku sektori asutuse kvalifitseeritud e-allkirja või kvalifitseeritud e-templit toetav kvalifitseeritud sertifikaat peab sisaldama sertifitseeritud atribuute automaatseks töötlemiseks sobivas formaadis:

i) näidates, et väljastav asutus on asutatud vastavalt siseriiklikule või liidu õigusele asutusena, mis vastutab autentse allika eest, mille alusel atribuutide elektrooniline tõend välja antakse, või asutusena, mis on määratud tegutsema selle asutuse nimel;

ii) esitades andmed, mis üheselt mõistetavalt tähistavad alapunktis i osutatud autentset allikat; ning

iii) määrates kindlaks alapunktis i osutatud siseriikliku või liidu õiguse.

2. Liikmesriik, kus artikli 3 punktis 45a osutatud avaliku sektori asutused on asutatud, tagab et atribuutide elektroonilisi tõendeid väljaandvad avaliku sektori asutused vastavad samaväärsele usaldusväärsuse tasemele kui kvalifitseeritud usaldusteenuse osutajad vastavalt artiklile 24.

2a. Liikmesriigid teavitavad artikli 3 punktis 45a osutatud avaliku sektori asutustest komisjoni. See teade hõlmab vastavushindamisasutuse väljastatud vastavushindamisaruannet, milles kinnitatakse, et käesoleva artikli lõigetes 1, 2 ja 6 sätestatud nõuded on täidetud. Komisjon teeb artikli 3 punktis 45a osutatud avaliku sektori asutuste loetelu turvalise kanali kaudu avalikkusele kättesaadavaks automaatseks töötlemiseks sobivas, elektrooniliselt allkirjastatud või e-templiga varustatud formaadis.

3 Kui autentse allika eest vastutava avaliku sektori asutuse poolt või nimel väljastatud elektrooniline atribuutide tõend pärast esialgset väljastamist tühistatakse, kaotab see kehtivuse alates tühistamise hetkest. Pärast tühistamist ei saa elektrooniline tõend oma endist staatust tagasi.

4. Autentse allika eest vastutava avaliku sektori asutuse poolt või nimel välja antud elektrooniline atribuutide tõend loetakse käesoleva artikli lõikes 1 sätestatud nõuetele vastavaks, kui see vastab lõikes 5 osutatud standarditele.

5. Kuue kuu jooksul pärast käesoleva määruse jõustumist kehtestab komisjon autentse allika eest vastutava avaliku sektori asutuse poolt või nimel välja antud elektrooniliste atribuutide tõendite tehnilised kirjeldused ja asjakohaste standardite viitenumbrid, võttes vastu artikli 6a lõikes 11 osutatud rakendusakti Euroopa digiidentiteeditaskute rakendamise kohta.

5a. Kuue kuu jooksul pärast käesoleva määruse jõustumist määrab komisjon kindlaks lõike 2a kohaldamisega seotud formaadid, menetlused, spetsifikatsioonid ja standardid, võttes vastu rakendusakti Euroopa digiidentiteeditaskute rakendamise kohta vastavalt artikli 6a lõikele 11.

6. Artikli 3 punktis 45a osutatud avaliku sektori asutused, kes väljastavad elektroonilisi atribuutide tõendeid, loovad liidese artikli 6a kohaselt pakutavate Euroopa digiidentiteeditaskute jaoks.

Artikkel 45e

Atribuutide elektrooniliste tõendite väljastamine Euroopa digiidentiteeditaskutele

Kvalifitseeritud elektrooniliste atribuutide tõendite pakkujad loovad liidese artikli 6a kohaselt pakutavate Euroopa digiidentiteeditaskute jaoks.

Artikkel 45f

Täiendavad eeskirjad elektroonilise atribuutide tõendamise teenuste osutamiseks

1. Kvalifitseeritud ja kvalifitseerimata elektroonilise atribuutide tõendamise teenuste osutajad ei tohi kombineerida selliste teenuste osutamisega seotud isikuandmeid enda või oma äripartnerite pakutavate muude teenustega seotud isikuandmetega.

2. Elektroonilise atribuutide tõendamise teenuste osutamisega seotud isikuandmeid hoitakse muudest atribuutide elektrooniliste tõendite pakkujate säilitatavatest andmetest loogiliselt eraldi.

4. Kvalifitseeritud elektroonilise atribuutide tõendamise teenuste osutajad rakendavad selliste teenuste osutamisel funktsioonipõhist eraldamist.

10. JAGU

ELEKTROONILISE ARHIVEERIMISE TEENUSED

Artikkel 45g

Elektroonilise arhiveerimise teenuse õiguslik toime

1. Elektroonilise arhiveerimise teenust kasutades säilitatavaid elektroonilisi andmeid ei tunnistata õiguslikult kehtetuks ega kohtumenetlustes tõenduskõlbmatuks ainuüksi seetõttu, et need on elektroonilised või et neid ei säilitata kvalifitseeritud elektroonilise arhiveerimise teenust kasutades.

2. Kvalifitseeritud elektroonilise arhiveerimise teenuse abil säilitatavate elektrooniliste andmete puhul kehtib niikaua, kui kvalifitseeritud usaldusteenuse osutaja neid säilitab, nende andmete tervikluse ja päritolu presumptsioon.

3. Ühe liikmesriigi kvalifitseeritud elektroonilise arhiveerimise teenust tunnustatakse kvalifitseeritud elektroonilise arhiveerimise teenusena kõikides liikmesriikides.

Artikkel 45ga

Kvalifitseeritud elektroonilise arhiveerimise teenustele esitatavad nõuded

1. Kvalifitseeritud elektroonilise arhiveerimise teenused peavad vastama järgmistele nõuetele:

   a) neid pakuvad kvalifitseeritud usaldusteenuse osutajad;

   b) nende puhul kasutatakse menetlusi ja tehnoloogiaid, millega on võimalik tagada elektrooniliste andmete säilivus ja loetavus ka pärast nende tehnoloogilise kehtivusaja lõppemist ja vähemalt kogu nende õigusliku või lepingujärgse säilitamisaja jooksul, säilitades samal ajal nende tervikluse ja päritolu;

c) nende puhul on tagatud, et elektroonilisi andmeid säilitatakse selliselt, et need on kaitstud kaotsimineku ja muutmise eest, välja arvatud muutused seoses andmekandja või andmete elektroonilise vorminguga;

d) need võimaldavad volitatud tuginevatel isikutel saada automaatselt aruande, mis kinnitab, et kvalifitseeritud elektroonilisest arhiivist saadud elektrooniliste andmete suhtes kehtib andmetervikluse presumptsioon nende säilitamisaja algusest kuni otsingu hetkeni. Nimetatud aruanne esitatakse usaldusväärsel ja tõhusal viisil ning sellel on kvalifitseeritud elektroonilise arhiveerimise teenuse osutaja kvalifitseeritud e-allkiri või kvalifitseeritud e-tempel.

2. 12 kuu jooksul pärast käesoleva määruse jõustumist kehtestab komisjon rakendusaktidega kvalifitseeritud elektroonilise arhiveerimise teenuste tehnilised kirjeldused ja asjakohaste standardite viitenumbrid. Kui kvalifitseeritud elektrooniline arhiiviteenus vastab kõnealustele tehnilistele kirjeldustele ja standarditele, loetakse kvalifitseeritud elektroonilise arhiveerimise teenustele esitatavad nõuded täidetuks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.

11. JAGU

ELEKTROONILISED REGISTRID

Artikkel 45h

Elektrooniliste registrite õiguslik toime

1. Elektroonilist registrit ei tunnistata õiguslikult kehtetuks ega kohtumenetlustes tõenduskõlbmatuks ainuüksi seetõttu, et see on elektroonilisel kujul või ei vasta kvalifitseeritud elektroonilistele registritele esitatavatele nõuetele.

2. Kvalifitseeritud elektroonilises registris sisalduvate andmekirjete puhul kehtib nende kordumatu ja täpse kronoloogilise järjestuse ning tervikluse presumptsioon.

3. Ühe liikmesriigi kvalifitseeritud elektroonilist registrit tunnustatakse kvalifitseeritud elektroonilise registrina kõikides liikmesriikides.

Artikkel 45i

Kvalifitseeritud elektroonilistele registritele esitatavad nõuded

1. Kvalifitseeritud elektroonilised registrid vastavad järgmistele nõuetele:

   a) need on loonud üks või mitu kvalifitseeritud usaldusteenuse osutajat;

   b) need teevad kindlaks registrisse kantud andmekirjete päritolu;

   c) need tagavad registrisse kantud andmekirjete kordumatu kronoloogilise järjestuse;

   d) neisse registreeritakse andmeid sellisel viisil, et kõik hilisemad andmete muudatused on kohe tuvastatavad, mis tagab andmete tervikluse ajas.

2. Kui elektrooniline register vastab lõikes 3 osutatud kirjeldustele ja standarditele, loetakse lõikes 1 sätestatud nõuded täidetuks.

3. Komisjon kehtestab rakendusaktidega kvalifitseeritud elektroonilise registri loomise ja toimimise tehnilised kirjeldused ja asjakohaste standardite viitenumbrid. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 48 lõikes 2 osutatud kontrollimenetlusega.“

40) Lisatakse artikkel 48a:

„Artikkel 48a

Aruandlusnõuded

1. Liikmesriigid tagavad statistika kogumise Euroopa digiidentiteeditaskute toimimise kohta niipea, kui neid nende territooriumil pakutakse.

2. Lõike 1 kohaselt kogutud statistika hõlmab järgmist:

a) füüsiliste ja juriidiliste isikute arv, kellel on kehtiv Euroopa digiidentiteeditasku;

b) Euroopa digiidentiteeditaskute kasutamist aktsepteerivate teenuste liik ja arv;

c) koondaruanne, mis sisaldab andmeid Euroopa digiidentiteeditasku kasutamist takistavate intsidentide kohta.

3. Lõikes 2 osutatud statistika tehakse üldsusele kättesaadavaks avatud ja üldkasutatavas masinloetavas vormingus.

4. Liikmesriigid esitavad komisjonile iga aasta 31. märtsiks aruande lõike 2 kohaselt kogutud statistika kohta.“

41) Artikkel 49 asendatakse järgmisega:

„*Artikkel 49*

Läbivaatamine

1. Komisjon vaatab läbi käesoleva määruse kohaldamise ja esitab Euroopa Parlamendile ja nõukogule selle kohta 36 kuu jooksul pärast määruse jõustumist aruande. Komisjon hindab eelkõige artikli 6 ja artikli 6db kohaldamisala ning seda, kas on asjakohane muuta käesoleva määruse kohaldamisala või selle erisätteid, võttes arvesse käesoleva määruse kohaldamisel saadud kogemusi ning klientidepoolset nõudlust ja tehnoloogia, turu ja õiguse arengut. Kui see on vajalik, lisatakse aruandele määruse muutmise ettepanekud.

2. Hindamisaruanne sisaldab hinnangut käesoleva määruse kohaldamisalasse kuuluvate Euroopa digiidentiteeditaskute kättesaadavuse ja kasutatavuse kohta ning hinnangut selle kohta, kas kõigil eraõiguslikel internetipõhise teenuse osutajatel, kes tuginevad kasutajate autentimisel kolmanda isiku e-identimise teenustele, on kohustus aktsepteerida Euroopa digiidentiteeditaskute kasutamist.

3. 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.“

42) Artikkel 51 asendatakse järgmisega:

„*Artikkel 51*

Üleminekumeetmed

1. Turvalised allkirja andmise vahendid, mille vastavus on kindlaks määratud vastavalt direktiivi 1999/93/EÜ artikli 3 lõikele 4, loetakse käesoleva määruse kohaselt jätkuvalt kvalifitseeritud e-allkirja andmise vahenditeks 36 kuu jooksul pärast käesoleva määruse jõustumist.

2. Direktiivi 1999/93/EÜ kohaselt füüsilistele isikutele väljastatud kvalifitseeritud sertifikaate käsitatakse käesoleva määruse kohaselt jätkuvalt e-allkirjade kvalifitseeritud sertifikaatidena 24 kuu jooksul pärast käesoleva määruse jõustumist.

2a. Kvalifitseeritud e-allkirja vahemaa tagant andmise ja e-templi vahemaa tagant loomise vahendite haldamist muude kvalifitseeritud usaldusteenuse osutajate poolt kui kvalifitseeritud usaldusteenuse osutajad, kes osutavad kvalifitseeritud usaldusteenuseid kvalifitseeritud e-allkirjade vahemaa tagant andmise ja e-templite vahemaa tagant loomise vahendite haldamiseks kooskõlas artiklitega 29a ja 39a, käsitatakse 24 kuu jooksul pärast käesoleva määruse jõustumist jätkuvalt nii, et kõnealuste haldusteenuste osutamiseks ei ole vaja saada kvalifitseeritud staatust.

2b. Kvalifitseeritud usaldusteenuse osutajad, kellele on käesoleva määruse alusel antud kvalifitseeritud staatus enne [muutmismääruse jõustumise kuupäev] ja kes kasutavad artikli 24 lõike 1 kohaseid kvalifitseeritud sertifikaatide väljastamisel kohaldatavaid identiteedi kontrollimise meetodeid, esitavad järelevalveasutusele artikli 24 lõike 1 nõuetele vastavust tõendava vastavushindamisaruande niipea kui võimalik ja hiljemalt 30 kuu möödumisel muutmismääruse jõustumisest. Kuni sellise vastavushindamisaruande esitamiseni ja selle hindamise lõpuleviimiseni järelevalveasutuse poolt võib kvalifitseeritud usaldusteenuse osutaja kasutada jätkuvalt määruse (EL) nr 910/2014 artikli 24 lõikes 1 sätestatud identiteedi kontrollimise meetodeid.“

43) I lisa muudetakse vastavalt käesoleva määruse I lisale;

44) II lisa asendatakse käesoleva määruse II lisas esitatud tekstiga;

45) III lisa muudetakse vastavalt käesoleva määruse III lisale;

46) IV lisa muudetakse vastavalt käesoleva määruse IV lisale;

47) lisatakse käesoleva määruse V lisas sätestatud uus V lisa;

48) käesolevale määrusele lisatakse uus VI lisa.

Artikkel 52

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

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel,

Euroopa Parlamendi nimel Nõukogu nimel

president eesistuja

I LISA

I lisa punkt i) asendatakse järgmisega:

„i) teave kvalifitseeritud sertifikaadi kehtivuse kohta või selle kohta, kus asuvad teenused, mida saab kasutada kvalifitseeritud sertifikaadi kehtivuse kohta teabe saamiseks;“.

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.

III LISA

III lisa punkt i) asendatakse järgmisega:

„i) teave kvalifitseeritud sertifikaadi kehtivuse kohta või selle kohta, kus asuvad teenused, mida saab kasutada kvalifitseeritud sertifikaadi kehtivuse kohta teabe saamiseks;“.

IV LISA

IV lisa punkt j) asendatakse järgmisega:

„j) teave kvalifitseeritud sertifikaadi kehtivuse kohta või kvalifitseeritud sertifikaadi kehtivuse kohta teavet saada võimaldavate teenuste asukoht.“.

V LISA

KVALIFITSEERITUD ATRIBUUTIDE TÕENDITELE ESITATAVAD NÕUDED

Kvalifitseeritud elektroonilised atribuutide tõendid sisaldavad järgmist:

e) vähemalt automaatseks töötlemiseks sobivas formaadis märge selle kohta, et tõend on väljastatud kvalifitseeritud elektroonilise atribuutide tõendina;

f) andmed, mis üheselt mõistetavalt tähistavad kvalifitseeritud elektroonilisi atribuutide tõendeid väljastavat kvalifitseeritud usaldusteenuse osutajat ning sisaldavad vähemalt selle liikmesriigi nime, kus teenuseosutaja on asutatud, ning

– juriidilise isiku puhul nimi ja asjakohasel juhul registrinumber, nagu see on esitatud ametlikes dokumentides,

– füüsilise isiku puhul isiku nimi;

g) andmed, mis üheselt mõistetavalt tähistavad üksust, kellele tõendatud atribuut viitab; kui kasutatakse varjunime, on varjunime kasutus selgesti näidatud;

h) tõendatud atribuut või atribuudid, sealhulgas vajaduse korral teave, mis on vajalik, et teha kindlaks nende atribuutide kohaldamisala;

i) üksikasjalikud andmed tõendi kehtivusaja alguse ja lõpu kohta;

j) tõendi identifitseerimiskood, mis peab olema igal kvalifitseeritud usaldusteenuse osutajal kordumatu, ja vajaduse korral märge tõendite süsteemi kohta, kuhu atribuutide tõend kuulub;

k) väljastava kvalifitseeritud usaldusteenuse osutaja kvalifitseeritud e-allkiri või kvalifitseeritud e-tempel;

l) koht, kus punktis g osutatud kvalifitseeritud e-allkirja või kvalifitseeritud e-templit toetav sertifikaat on tasuta kättesaadav;

m) teave kvalifitseeritud tõendi kehtivuse kohta või selle kohta, kus asuvad teenused, mida saab kasutada kvalifitseeritud tõendi kehtivuse kohta teabe saamiseks.

VI LISA

MIINIMUMATRIBUUTIDE LOETELU

Vastavalt artiklile 45 d tagavad liikmesriigid, et võetakse meetmeid, et võimaldada elektrooniliste atribuutide tõendite kvalifitseeritud pakkujatel kontrollida kasutaja taotlusel elektrooniliste vahendite abil järgmiste atribuutide autentsust asjaomasest autentsest allikast riiklikul tasandil või määratud vahendajate kaudu, kes on siseriikliku või liidu õiguse kohaselt tunnustatud ja juhtudel, kui need atribuudid põhinevad avaliku sektori autentsetel allikatel:

1. aadress;
2. vanus;
3. sugu;
4. perekonnaseis;
5. perekonna koosseis;
6. kodakondsus;
7. haridusalane kvalifikatsioon, kraadid ja diplomid;
8. kutsekvalifikatsioon, kutsenimetused ja litsentsid;
9. avalikud load ja litsentsid;
10. finantsandmed ja ettevõtte andmed.

VII LISA

AUTENTSE ALLIKA EEST VASTUTAVA AVALIKU SEKTORI ASUTUSE POOLT VÕI NIMEL VÄLJA ANTUD ELEKTROONILISTELE ATRIBUUTIDE TÕENDITELE ESITATAVAD NÕUDED

Autentse allika eest vastutava avaliku sektori asutuse poolt või nimel välja antud elektrooniline atribuutide tõend hõlmab järgmist:

a) vähemalt automaatseks töötlemiseks sobivas formaadis märge selle kohta, et tõend on väljastatud autentse allika eest vastutava avaliku sektori asutuse poolt või nimel välja antud elektroonilise atribuutide tõendina;
b) andmed, mis üheselt mõistetavalt tähistavad atribuutide elektroonilisi tõendeid väljastavat avaliku sektori asutust ning sisaldavad vähemalt selle liikmesriigi nime, kus see avaliku sektori asutus on asutatud, asutuse nime ja asjakohasel juhul registrinumbrit, nagu see on esitatud ametlikes dokumentides;
c) andmed, mis üheselt mõistetavalt tähistavad üksust, kellele tõendatud atribuut viitab; kui kasutatakse varjunime, on varjunime kasutus selgesti näidatud;
d) tõendatud atribuut või atribuudid, sealhulgas vajaduse korral teave, mis on vajalik, et teha kindlaks nende atribuutide kohaldamisala;
e) üksikasjalikud andmed tõendi kehtivusaja alguse ja lõpu kohta;
f) tõendi identifitseerimiskood, mis peab olema igal väljastaval avaliku sektori asutusel kordumatu, ja vajaduse korral märge tõendite süsteemi kohta, kuhu atribuutide tõend kuulub;
g) väljastava asutuse kvalifitseeritud e-allkiri või kvalifitseeritud e-tempel;
h) koht, kus punktis g osutatud kvalifitseeritud e-allkirja või kvalifitseeritud e-templit toetav sertifikaat on tasuta kättesaadav;
i) teave tõendi kehtivuse kohta või selle kohta, kus asuvad teenused, mida saab kasutada tõendi kehtivuse kohta teabe saamiseks.

_____