



EUROOPAN UNIONI

EUROOPAN PARLAMENTTI

NEUVOSTO

**Bryssel, 11. huhtikuuta 2024
(OR. en)**

**2021/0136(COD)
LEX 2318**

**PE-CONS 68/1/23
REV 1**

**TELECOM 351
COMPET 1163
MI 1028
DATAPROTECT 329
JAI 1550
CODEC 2237**

**EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS
ASETUKSEN (EU) N:o 910/2014 MUUTTAMISESTA
EUROOPPALAISEN DIGITAALISEN IDENTITEETIN KEHYKSEN
VAHVISTAMISEN OSALTA**

**EUROOPAN PARLAMENTIN JA NEUVOSTON
ASETUS (EU) 2024/...,**

annettu 11 päivänä huhtikuuta 2024,

**asetuksen (EU) N:o 910/2014 muuttamisesta
eurooppalaisen digitaalisen identiteetin kehyksen vahvistamisen osalta**

EUROOPAN PARLAMENTTI JA EUROOPAN UNIONIN NEUVOSTO, jotka

ottavat huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 114 artiklan,

ottavat huomioon Euroopan komission ehdotuksen,

sen jälkeen kun esitys lainsäätämisyksessä hyväksyttäväksi säädökseksi on toimitettu kansallisille parlamenteille,

ottavat huomioon Euroopan talous- ja sosiaalikomitean lausunnon¹,

ottavat huomioon alueiden komitean lausunnon²,

noudattavat tavallista lainsäätämisyksitystä³,

¹ EUVL C 105, 4.3.2022, s. 81.

² EUVL C 61, 4.2.2022, s. 42.

³ Euroopan parlamentin kanta, vahvistettu 29. helmikuuta 2024 (ei vielä julkaistu virallisessa lehdessä), ja neuvoston päätös, tehty 26. maaliskuuta 2024.

sekä katsovat seuraavaa:

- (1) Komission 19 päivänä helmikuuta 2020 antamassa tiedonannossa ”Euroopan digitaalista tulevaisuutta rakentamassa” ilmoitetaan Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014⁴ tarkistamisesta sen tehokkuuden parantamiseksi, sen hyötyjen laajentamiseksi yksityiselle sektorille ja luotettavien digitaalisten identiteettien edistämiseksi kaikille eurooppalaisille.
- (2) Eurooppa-neuvosto kehotti 1 ja 2 päivänä lokakuuta 2020 antamissaan päätelmissä komissiota ehdottamaan unionin laajuisen suojatun julkisen sähköisen tunnistamisjärjestelmän kehityksen kehittämistä, yhteentoimivat digitaaliset allekirjoitukset mukaan luettuina, jotta ihmiset voivat valvoa verkkohenkilöllisyyttään ja verkossa olevia tietojaan ja jotta heillä on pääsy julkisiin, yksityisiin ja rajatylittäviin digitaalisiin palveluihin.
- (3) Euroopan parlamentin ja neuvoston päätöksellä (EU) 2022/2481⁵ perustetussa digitaalinen vuosikymmen 2030 -ohjelmassa vahvistetaan unionin kehityksen päämäärät ja digitalisaatiotavoitteet, joiden tarkoituksena on johtaa vuoteen 2030 mennessä sellaisen luotettavan, vapaaehtoisen ja käyttäjän määräysvallassa olevan digitaalisen identiteetin laajamittaiseen käyttöönottoon, joka tunnustetaan kaikkialla unionissa ja jonka avulla jokainen käyttäjä voi hallita omia tietojaan sähköisessä vuorovaikutuksessa.

⁴ Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta (EUVL L 257, 28.8.2014, s. 73).

⁵ Euroopan parlamentin ja neuvoston päätös (EU) 2022/2481, annettu 14 päivänä joulukuuta 2022, digitaalinen vuosikymmen 2030 -ohjelman perustamisesta (EUVL L 323, 19.12.2022, s. 4).

- (4) Euroopan parlamentin, neuvoston ja komission antamassa eurooppalaisessa julistuksessa digitaalisen vuosikymmenen digitaalisista oikeuksista ja periaatteista⁶, jäljempänä 'julistus', korostetaan jokaisen kansalaisen oikeutta käyttää turvallisia ja sisäänrakennetusti yksityisyyttä suojaavia digiteknologioita, -tuotteita ja -palveluja. Tähän sisältyy sen varmistaminen, että kaikille unionissa asuville henkilöille tarjotaan esteetön, turvallinen ja luotettava digitaalinen identiteetti, joka mahdollistaa monenlaisten verkkopalvelujen ja verkon ulkopuolisten palvelujen käytön, jotka on suojattu kyberturvallisuusriskeiltä ja kyberrikollisuudelta, muun muassa tietoturvaloukkauksilta, identiteettivarkauksilta tai manipuloinnilta. Julistuksessa todetaan myös, että jokaisella on oikeus henkilötietojensa suojaan. Kyseiseen oikeuteen kuuluu sen hallinta, miten tietoja käytetään ja kenen kanssa ne jaetaan.
- (5) Unionin kansalaisilla ja unionissa asuvilla henkilöillä olisi oltava oikeus digitaaliseen identiteettiin, joka on heidän yksinomaisessa määräysvallassaan ja jonka avulla he voivat käyttää oikeuksiaan digitaalisessa ympäristössä ja osallistua digitaalitalouteen. Tämän tavoitteen saavuttamiseksi olisi vahvistettava eurooppalainen digitaalisen identiteetin kehys, jonka avulla unionin kansalaiset ja unionissa asuvat henkilöt voivat käyttää julkisia ja yksityisiä verkkopalveluja ja verkon ulkopuolisia palveluja kaikkialla unionissa.
- (6) Yhdenmukaistetun digitaalisen identiteetin kehysten olisi tuettava digitaalisesti yhdentyneemmän unionin luomista vähentämällä digitaalisia esteitä jäsenvaltioiden väliltä ja antamalla unionin kansalaisille ja unionissa asuville henkilöille mahdollisuuden hyötyä digitalisaation eduista lisäten samalla avoimuutta ja heidän oikeuksiensa suojelua.

⁶ EUVL C 23, 23.1.2023, s. 1.

- (7) Omaksumalla yhdenmukaisempi lähestymistapa sähköiseen tunnistamiseen voitaisiin vähentää riskejä ja kustannuksia, joita aiheutuu toisistaan poikkeavien kansallisten ratkaisujen käytöstä tai joissakin jäsenvaltioissa tällaiseen sähköiseen tunnistamiseen liittyvien ratkaisujen puutteesta johtuvasta nykyisestä hajanaisuudesta. Tällaisen lähestymistavan olisi vahvistettava sisämarkkinoita antamalla unionin kansalaisille, kansallisessa lainsäädännössä määritellyille unionissa asuville henkilöille sekä yrityksille mahdollisuus tunnistautua ja todentaa henkilöllisyytensä verkossa ja verkon ulkopuolella turvallisella, luotettavalla, käyttäjäystävällisellä, helppokäyttöisellä, saavutettavalla ja yhdenmukaisella tavalla kaikkialla unionissa. Eurooppalaisen digitaalisen identiteetin lompakon olisi tarjottava luonnollisille henkilöille ja oikeushenkilöille kaikkialla unionissa yhdenmukaistettu sähköisen tunnistamisen menetelmä, jonka avulla nämä voivat todentaa ja jakaa henkilöllisyyteensä liittyviä tietoja. Kaikilla olisi oltava julkisten ja yksityisten palvelujen turvallinen käyttömahdollisuus, joka perustuu parannettuun luottamuspalvelujen ekosysteemiin sekä varmennettuihin todisteisiin henkilöllisyydestä ja sähköisiin attribuuttitodistuksiin, kuten akateemisiin tutkintotodistuksiin, mukaan lukien yliopistotutkinnot, tai muihin koulutuksesta tai ammattipätevyydestä annettuihin asiakirjoihin. Eurooppalaisessa digitaalisen identiteetin kehyksessä pyritään siirtymään pelkästään kansallisten digitaalisten identiteettiratkaisujen käytöstä kaikkialla unionissa voimassa oleviin ja oikeudellisesti tunnustettuihin sähköisiin attribuuttitodistuksiin. Sähköisten attribuuttitodistusten tarjoajilla olisi oltava selkeät ja yhdenmukaiset säännöt, samalla kun julkishallintojen olisi voitava luottaa tietystä muodossa oleviin sähköisiin asiakirjoihin.

- (8) Useat jäsenvaltiot ovat toteuttaneet ja käyttävät sähköisen tunnistamisen menetelmiä, jotka unionissa toimivat palveluntarjoajat hyväksyvät. Lisäksi on tehty investointeja sekä kansallisiin että rajatylittäviin ratkaisuihin asetuksen (EU) N:o 910/2014 perusteella, mukaan lukien ilmoitettujen sähköisen tunnistamisen järjestelmien yhteentoimivuus kyseisen asetuksen nojalla. Jotta voidaan varmistaa eurooppalaisten digitaalisen identiteetin lompakoiden täydentävyys ja nopea käyttöönotto ilmoitettujen sähköisen tunnistamisen menetelmien nykyisten käyttäjien keskuudessa ja minimoida nykyisiin palveluntarjoajiin kohdistuvat vaikutukset, eurooppalaisten digitaalisen identiteetin lompakoiden odotetaan käyttävän hyväksi nykyisistä sähköisen tunnistamisen menetelmistä saatuja kokemuksia sekä unionin ja kansallisella tasolla käyttöönotettua ilmoitettujen sähköisen tunnistamisen järjestelmien infrastruktuuria.
- (9) Kaikkiin asetuksen (EU) N:o 910/2014 mukaisiin henkilötietojen käsittelytoimiin sovelletaan Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679⁷ ja tarvittaessa Euroopan parlamentin ja neuvoston direktiiviä 2002/58/EY⁸. Tässä asetuksessa säädetyn yhteentoimivuuskehityksen mukaiset ratkaisut ovat myös kyseisten sääntöjen mukaisia. Unionin tietosuojalainsäädännössä säädetään tietosuojaperiaatteista, kuten tietojen minimoinnin ja käyttötarkoituksen rajoittamisen periaatteesta, sekä velvoitteista, joita ovat esimerkiksi sisäänrakennettu ja oletusarvoinen tietosuoja.

⁷ Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EUVL L 119, 4.5.2016, s. 1).

⁸ Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi) (EYVL L 201, 31.7.2002, s. 37).

- (10) Unionin yritysten kilpailukyvyn tukemiseksi sekä verkkopalvelujen että verkon ulkopuolisten palvelujen tarjoajien olisi voitava käyttää kaikkialla unionissa tunnustettuja digitaalisia identiteettiratkaisuja riippumatta siitä, missä jäsenvaltiossa ne on tarjottu, ja hyötyä näin yhdenmukaisesta unionin lähestymistavasta luottamukseen, turvallisuuteen ja yhteentoimivuuteen. Sekä käyttäjien että palveluntarjoajien olisi voitava hyötyä siitä, että sähköisille attribuuttitodistuksille annetaan sama oikeudellinen arvo kaikkialla unionissa. Yhdenmukaistetun digitaalisen identiteetin kehityksen tarkoituksena on luoda taloudellista arvoa parantamalla tavaroiden ja palvelujen saatavuutta ja vähentämällä merkittävästi sähköisiin tunnistus- ja todentamismenettelyihin liittyviä toimintakustannuksia, joita syntyy esimerkiksi aloitettaessa uusia käyttösuhteita, sekä vähentämällä identiteettivarkauksien, tietovarkauksien ja verkkopetosten kaltaisen kyberrikollisuuden mahdollisuuksia, mikä edistää tehokkuutta ja unionin mikroyritysten ja pienten ja keskisuurten yritysten (pk-yritysten) turvallista digitalisaatiota.
- (11) Eurooppalaisten digitaalisen identiteetin lompakoiden olisi helpotettava yhden kerran periaatteen soveltamista, mikä vähentää unionin kansalaisille ja unionissa asuville henkilöille sekä kaikkialla unionissa toimiville yrityksille aiheutuvaa hallinnollista taakkaa ja tukee näiden rajatylittävää liikkumista sekä edistää yhteentoimivien sähköisten viranomaispalvelujen kehittämistä kaikkialla unionissa.

- (12) Tämän asetuksen täytäntöönpanon yhteydessä tapahtuvaan henkilötietojen käsittelyyn sovelletaan Euroopan parlamentin ja neuvoston asetuksia (EU) 2016/679 ja (EU) 2018/1725⁹ sekä direktiiviä 2002/58/EY. Sen vuoksi tässä asetuksessa olisi säädettävä erityisistä suojatoimista, joilla estetään sähköisen tunnistamisen menetelmien ja sähköisten attribuuttitodistusten tarjoajia yhdistämästä muiden palvelujen tarjoamisen yhteydessä saatuja henkilötietoja tämän asetuksen soveltamisalaan kuuluvien palvelujen tarjoamista varten käsiteltäviin henkilötietoihin. Eurooppalaisten digitaalisen identiteetin lompakoiden tarjoamiseen liittyvät henkilötiedot olisi pidettävä loogisesti erillään kaikista muista tiedoista, joita eurooppalaisen identiteetin lompakon tarjoajan hallussa on. Tämän asetuksen ei olisi estettävä eurooppalaisten digitaalisen identiteetin lompakoiden tarjoajia soveltamasta henkilötietojen suojaa parantavia teknisiä lisätoimenpiteitä, kuten eurooppalaisten digitaalisen identiteetin lompakoiden tarjoamiseen liittyvien henkilötietojen fyysistä erottamista kaikista muista lompakon tarjoajan hallussa olevista tiedoista. Tässä asetuksessa täsmennetään myös käyttötarkoituksen rajoittamista, tietojen minimointia sekä sisäänrakennettua ja oletusarvoista tietosuojaa koskevien periaatteiden soveltamista, sanotun kuitenkin rajoittamatta asetuksen (EU) 2016/679 soveltamista.

⁹ Euroopan parlamentin ja neuvoston asetus (EU) 2018/1725, annettu 23 päivänä lokakuuta 2018, luonnollisten henkilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä asetuksen (EY) N:o 45/2001 ja päätöksen N:o 1247/2002/EY kumoamisesta (EUVL L 295, 21.11.2018, s. 39).

- (13) Eurooppalaisissa digitaalisen identiteetin lompakoissa olisi oltava sisäänrakennettuna toimintona yhteinen ohjauspaneeli, jotta varmistetaan suurempi avoimuus ja yksityisyys ja se, että käyttäjät voivat hallita henkilötietojaan. Kyseisen toiminnon olisi tarjottava helppo ja käyttäjäystävällinen rajapinta, joka antaa yleiskuvan kaikista luottavista osapuolista, joiden kanssa käyttäjä jakaa tietoja, mukaan lukien attribuutit, sekä kunkin luottavan osapuolen kanssa jaettujen tietojen tyypistä. Sen avulla käyttäjien olisi voitava jäljittää kaikki eurooppalaisia digitaalisen identiteetin lompakkoja käyttäen toteutetut transaktiot ja saamaan niistä vähintään seuraavat tiedot: transaktion aika ja päivämäärä, vastapuolen tunnistetiedot, pyydetty henkilötiedot ja jaetut tiedot. Nämä tiedot olisi tallennettava, vaikka transaktio ei toteutuisi. Transaktiohistorian sisältämien tietojen aitoutta ei saisi olla mahdollista kiistää. Tällaisen toiminnon olisi oltava aktivoituna oletusarvoisesti. Sen olisi mahdollistettava se, että käyttäjät voivat helposti pyytää, että luottava osapuoli poistaa henkilötietoja välittömästi asetuksen (EU) 2016/679 17 artiklan mukaisesti ja raportoida vaivattomasti luottavasta osapuolesta sen jäsenvaltion kansalliselle toimivaltaiselle tietosuojaviranomaiselle, jossa väitetysti lainvastainen tai epäilyttävä henkilötietopyyntö on saatu, suoraan eurooppalaisen digitaalisen identiteetin lompakon kautta.
- (14) Jäsenvaltioiden olisi sisällytettävä eurooppalaiseen digitaalisen identiteetin lompakkoon erilaisia yksityisyyttä suojaavia tekniikoita, kuten nollatietotodiste. Tällaisten salausmenetelmien ansiosta luottava osapuoli voi validoida henkilön tunnistetietoihin ja attribuuttitodistukseen perustuvan lausuman totuudenmukaisuuden paljastamatta mitään kyseisen lausuman perustana olevia tietoja ja säilyttäen siten käyttäjän yksityisyyden.

- (15) Tässä asetuksessa määritellään yhdenmukaistetut edellytykset kehysten vahvistamiseksi jäsenvaltioiden tarjoamia eurooppalaisia digitaalisen identiteetin lompakoita varten. Kaikille unionin kansalaisille ja kansallisessa lainsäädännössä määritellyille unionissa asuville henkilöille olisi annettava mahdollisuus pyytää, valita, yhdistää, tallentaa, poistaa, jakaa ja esittää turvallisesti henkilöllisyyteensä liittyviä tietoja ja pyytää henkilötietojensa poistamista käyttäjäystävällisellä ja helppokäyttöisellä tavalla käyttäjän yksinomaisessa valvonnassa siten, että samalla mahdollistetaan henkilötietojen valikoiva luovuttaminen. Tässä asetuksessa otetaan huomioon yhteiset eurooppalaiset arvot ja kunnioitetaan perusoikeuksia, oikeudellisia takeita ja vastuuta ja suojellaan siten demokraattisia yhteiskuntia, unionin kansalaisia ja unionissa asuvia henkilöitä. Kyseisten tavoitteiden saavuttamiseksi käytettäviä tekniikoita olisi kehitettävä siten, että tavoitteena on mahdollisimman korkeatasoinen turvallisuus, yksityisyys, käyttäjäystävällisyys, saavutettavuus, laaja käytettävyys ja saumaton yhteentoimivuus. Jäsenvaltioiden olisi varmistettava, että kaikilla niiden kansalaisilla ja asukkailla on yhtäläinen mahdollisuus käyttää sähköistä tunnistamista. Jäsenvaltioiden ei olisi suoraan eikä välillisesti rajoitettava julkisten tai yksityisten palvelujen saatavuutta sellaisten luonnollisten henkilöiden tai oikeushenkilöiden osalta, jotka päättävät olla käyttämättä eurooppalaisia digitaalisen identiteetin lompakoita, ja niiden olisi asetettava saataville asianmukaisia vaihtoehtoisia ratkaisuja.
- (16) Jäsenvaltioiden olisi hyödynnettävä tämän asetuksen tarjoamia mahdollisuuksia tarjotakseen omalla vastuullaan eurooppalaisia digitaalisen identiteetin lompakoita alueellaan asuvien luonnollisten henkilöiden ja oikeushenkilöiden käyttöön. Jotta jäsenvaltioille voitaisiin tarjota joustavuutta ja hyödyntää uusinta teknologiaa, tämän asetuksen olisi mahdollistettava se, että jäsenvaltio tarjoaa eurooppalaisia digitaalisen identiteetin lompakoita suoraan, niitä tarjotaan jäsenvaltion toimeksiannosta tai niitä tarjotaan jäsenvaltiosta riippumatta, mutta kyseinen jäsenvaltio tunnustaa ne.

- (17) Luottavien osapuolten olisi toimitettava rekisteröintiä varten tarvittavat tiedot niiden sähköistä tunnistamista ja todentamista varten eurooppalaiseen digitaalisen identiteetin lompakoihin. Ilmoittaessaan eurooppalaisen digitaalisen identiteetin lompakon suunnitellusta käytöstään luottavien osapuolten olisi annettava tiedot mahdollisista tiedoista, joita ne pyytävät palvelujensa tarjoamiseksi, ja pyynnön syy. Luottavan osapuolen rekisteröinti helpottaa jäsenvaltioiden suorittamia tarkastuksia, jotka koskevat luottavien osapuolten toiminnan lainmukaisuutta unionin oikeuden mukaisesti. Tässä asetuksessa säädetty rekisteröintivelvollisuus ei saisi vaikuttaa muussa unionin oikeudessa tai kansallisessa lainsäädännössä säädettyihin velvollisuuksiin, kuten tietoihin, jotka on asetuksen (EU) 2016/679 nojalla annettava rekisteröidyille. Luottavien osapuolten olisi noudatettava kyseisen asetuksen 35 ja 36 artiklan tarjoamia suojatoimia erityisesti tekemällä tietosuojaa koskevia vaikutustenarviointeja ja kuulemalla toimivaltaisia tietosuojaviranomaisia ennen tietojen käsittelyä, jos tietosuojaa koskevat vaikutustenarvioinnit osoittavat, että käsittely aiheuttaisi suuren riskin. Tällaisten suojatoimien olisi tuettava luottavien osapuolten toteuttamaa henkilötietojen laillista käsittelyä etenkin erityisten tietoryhmien, kuten terveystietojen, osalta. Luottavien osapuolten rekisteröinnin tarkoituksena on lisätä avoimuutta ja luottamusta eurooppalaisten digitaalisen identiteetin lompakoiden käyttöön. Rekisteröinnin olisi oltava kustannustehokasta ja oikeassa suhteessa siihen liittyviin riskeihin, jotta varmistetaan, että palveluntarjoajat ottavat sen käyttöön. Tässä yhteydessä rekisteröinnissä olisi mahdollistettava automatisoitujen menettelyjen käyttö, mukaan lukien se, että jäsenvaltiot luottavat olemassa oleviin rekistereihinsä ja käyttävät niitä, eikä siihen saisi sisältyä ennakkohyväksyntämenettelyä. Rekisteröintimenettelyn olisi mahdollistettava erilaiset käyttötapaukset, jotka voivat vaihdella toimintatavan (joko verkossa tai verkon ulkopuolella) tai niiden laitteiden todentamisvaatimuksen osalta, jotka pystyvät toimimaan yhdessä eurooppalaisen digitaalisen identiteetin lompakon kanssa. Rekisteröinnin olisi koskettava yksinomaan luottavia osapuolia, jotka tarjoavat palveluja digitaalisen vuorovaikutuksen keinoin.

- (18) Unionin kansalaisten ja unionissa asuvien henkilöiden suojaaminen eurooppalaisten digitaalisen identiteetin lompakoiden luvattomalta tai vilpilliseltä käytöltä on erittäin tärkeää, jotta voidaan varmistaa luottamus eurooppalaisiin digitaalisen identiteetin lompakoihin ja edistää niiden laajaa käyttöönottoa. Käyttäjät olisi suojattava tehokkaasti tällaista väärinkäyttöä vastaan. Erityisesti silloin, kun kansallinen oikeusviranomainen vahvistaa jonkin toisen menettelyn yhteydessä tosiseikat, jotka muodostavat perustan eurooppalaisen digitaalisen identiteetin lompakon vilpilliselle tai muulla tavoin laittomalle käytölle, eurooppalaisen digitaalisen identiteetin lompakon tarjoajista vastaavien valvontaelinten olisi ilmoituksen saatuaan toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että luottavan osapuolen rekisteröinti ja luottavien osapuolten sisällyttäminen todentamismekanismiin peruutetaan tai keskeytetään, kunnes ilmoittamisesta vastaava viranomainen vahvistaa, että havaitut sääntöjenvastaisuudet on korjattu.

- (19) Kaikkien eurooppalaisten digitaalisen identiteetin lompakoiden olisi annettava käyttäjille mahdollisuus sähköiseen tunnistautumiseen ja todentamiseen verkossa ja verkon ulkopuolella yli rajojen, jotta he voivat käyttää laajaa valikoimaa julkisia ja yksityisiä palveluja. Eurooppalaiset digitaalisen identiteetin lompakot voivat palvella myös julkishallintojen, kansainvälisten järjestöjen ja unionin toimielinten, elinten, laitosten ja virastojen institutionaalisia tarpeita, sanotun kuitenkin rajoittamatta jäsenvaltioiden oikeuksia siltä osin kuin on kyse niiden kansalaisten ja asukkaiden tunnistamisesta. Verkon ulkopuolinen todentaminen olisi tärkeää monilla aloilla, mukaan lukien terveydenhoitoala, joilla palveluja tarjotaan usein henkilökohtaisen vuorovaikutuksen kautta. Myös sähköisissä lääkemääräyksissä olisi voitava luottaa QR-koodeihin tai vastaaviin teknologioihin aitouden todentamiseksi. Sähköisen tunnistamisen järjestelmiä koskevan korkean varmuustason varmistamiseksi eurooppalaisissa digitaalisen identiteetin lompakoissa olisi hyödynnettävä väärinkäytöltä suojattujen ratkaisujen, kuten turvatekijöiden, tarjoamia mahdollisuuksia tämän asetuksen mukaisten turvallisuusvaatimusten noudattamiseksi. Eurooppalaisten digitaalisen identiteetin lompakoiden olisi myös annettava käyttäjille mahdollisuus luoda ja käyttää hyväksytyjä sähköisiä allekirjoituksia ja leimoja, jotka hyväksytään kaikkialla unionissa. Kun luonnollisten henkilöiden eurooppalaisen digitaalisen identiteetin lompakon käyttösuhde on aloitettu, heidän olisi voitava käyttää eurooppalaista digitaalisen identiteetin lompakkoa allekirjoittamiseen hyväksytyillä sähköisillä allekirjoituksilla oletusarvoisesti ja maksutta ilman muita hallinnollisia menettelyjä. Käyttäjien olisi voitava allekirjoittaa tai leimata omaehtoisia ilmoituksia tai attribuutteja. Jotta kansalaisille ja yrityksille kaikkialla unionissa voidaan tuottaa yksinkertaistamisesta ja kustannussäästöistä koituvia hyötyjä, myös mahdollistamalla edustusvaltuudet ja sähköiset valtuutukset, jäsenvaltioiden olisi tarjottava yhteisiin standardeihin ja teknisiin eritelmiin perustuvia eurooppalaisia digitaalisen identiteetin lompakkoja saumattoman yhteentoimivuuden varmistamiseksi, tietoturvan parantamiseksi asianmukaisesti ja kyberhyökkäysten sietokyvyn vahvistamiseksi, millä pienennetään digitalisaatiosta unionin kansalaisille, unionissa asuville henkilöille ja yrityksille mahdollisesti koituvia riskejä merkittävästi.

Ainoastaan jäsenvaltioiden toimivaltaiset viranomaiset voivat tarjota korkean luottamustason henkilön henkilöllisyyden selvittämisessä ja siten antaa takeet siitä, että henkilö, joka väittää tai esittää olevansa tietty henkilö, on todellisuudessa se, kuka hän väittää olevansa. Siksi eurooppalaisten digitaalisen identiteetin lompakoiden tarjonnan olisi perustuttava unionin kansalaisten, unionissa asuvien henkilöiden tai oikeushenkilöiden oikeudelliseen identiteettiin. Oikeudellisen identiteetin käyttäminen ei saisi estää eurooppalaisten digitaalisen identiteetin lompakkojen käyttäjiä käyttämästä palveluja pseudonyymillä, jos todentamiseen ei liity lakisääteinen vaatimus oikeudellisesta identiteetistä. Luottamusta eurooppalaisiin digitaalisen identiteetin lompakoihin parantaisi se, että niitä tarjoavien ja hallinnoivien osapuolten edellytetään toteuttavan asianmukaisia teknisiä ja organisatorisia toimenpiteitä sen varmistamiseksi, että turvallisuuden taso on mahdollisimman korkea ja oikeassa suhteessa luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuviin riskeihin asetuksen (EU) 2016/679 mukaisesti.

- (20) Hyväksytyyn sähköisen allekirjoituksen käytön olisi oltava maksutonta kaikille luonnollisille henkilöille muihin kuin ammatillisiin tarkoituksiin. Jäsenvaltioiden olisi voitava säätää toimenpiteistä, joilla estetään luonnollisia henkilöitä käyttämästä hyväksytyjä sähköisiä allekirjoituksia ammatillisiin tarkoituksiin maksutta, ja joilla varmistetaan, että tällaiset toimenpiteet ovat oikeassa suhteessa tunnistettuihin riskeihin ja perusteltuja.

- (21) On hyödyllistä helpottaa eurooppalaisten digitaalisen identiteetin lompakoiden käyttöönottoa ja käyttöä integroimalla ne saumattomasti julkisten ja yksityisten digitaalisten palvelujen ekosysteemiin, joka on jo pantu täytäntöön kansallisella, paikallisella tai alueellisella tasolla. Kyseisen tavoitteen saavuttamiseksi jäsenvaltioiden olisi voitava säätää oikeudellisista ja organisatorisista toimenpiteistä, joilla lisätään joustavuutta eurooppalaisten digitaalisen identiteetin lompakoiden tarjoajien näkökulmasta ja luodaan edellytykset muillekin kuin tässä asetuksessa säädetyille eurooppalaisten digitaalisen identiteetin lompakoiden toiminnoille, muun muassa parantamalla yhteentoimivuutta olemassa olevien kansallisten sähköisen tunnistamisen menetelmien kanssa. Tällaiset lisätoiminnot eivät saisi millään tavoin haitata tässä asetuksessa säädettyjen eurooppalaisten digitaalisen identiteetin lompakoiden ydintoimintojen tarjoamista eivätkä antaa olemassa oleville kansallisille ratkaisuille etusijaa eurooppalaisiin digitaalisen identiteetin lompakoihin nähden. Koska tällaiset lisätoiminnot menevät tätä asetusta pidemmälle, niihin ei sovelleta tässä asetuksessa vahvistettuja säännöksiä, jotka koskevat eurooppalaisten digitaalisen identiteetin lompakoiden rajatylittävää käyttöä.
- (22) Eurooppalaisten digitaalisen identiteetin lompakkojen olisi sisällettävä toiminto, jolla muodostetaan käyttäjän valitsemia ja hallinnoimia pseudonyymejä henkilöllisyyden todentamiseksi verkkopalveluja käytettäessä.
- (23) Turvallisuuden ja luotettavuuden korkean tason saavuttamiseksi tässä asetuksessa vahvistetaan eurooppalaisia digitaalisen identiteetin lompakkoja koskevat vaatimukset. Jäsenvaltioiden nimeämien akkreditoitujen vaatimustenmukaisuuden arviointilaitosten olisi sertifioitava se, että eurooppalaiset digitaalisen identiteetin lompakot ovat näiden vaatimusten mukaisia.

- (24) Toisistaan poikkeavien lähestymistapojen välttämiseksi ja tässä asetuksessa säädettyjen vaatimusten täytäntöönpanon yhdenmukaistamiseksi komission olisi eurooppalaisten digitaalisen identiteetin lompakkojen sertifiointiseksi annettava täytäntöönpanosäädöksiä, joissa vahvistetaan luettelo viitestandardeista ja tarvittaessa vahvistetaan eritelmiä ja menettelyjä kyseisten vaatimusten yksityiskohtaisten teknisten eritelmien ilmaisemiseksi. Siltä osin kuin sen sertifiointi, ovatko eurooppalaiset digitaalisen identiteetin lompakot merkityksellisten kyberturvallisuusvaatimusten mukaisia, ei kuulu tässä asetuksessa tarkoitettujen olemassa olevien kyberturvallisuuden sertifiointijärjestelmien piiriin, ja siltä osin kuin on kyse eurooppalaisiin digitaalisen identiteetin lompakoihin liittyvistä muista kuin kyberturvallisuusvaatimuksista, jäsenvaltioiden olisi perustettava kansallisia sertifiointijärjestelmiä tässä asetuksessa vahvistettujen ja sen nojalla hyväksytyjen yhdenmukaistettujen vaatimusten mukaisesti. Jäsenvaltioiden olisi toimitettava luonnoksensa kansallisiksi sertifiointijärjestelmiksi eurooppalaiselle digitaalisen identiteetin yhteistyöryhmälle, jonka olisi voitava antaa lausuntoja ja suosituksia.
- (25) Tässä asetuksessa vahvistettujen kyberturvallisuusvaatimusten noudattamisen sertifiointiin olisi mahdollisuuksien mukaan perustuttava asiaankuuluviin eurooppalaisiin kyberturvallisuuden sertifiointijärjestelmiin, jotka on perustettu Euroopan parlamentin ja neuvoston asetuksella (EU) 2019/881¹⁰, jolla perustetaan vapaaehtoinen eurooppalainen kyberturvallisuuden sertifiointikehys tieto- ja viestintätekniikan tuotteille, prosesseille ja palveluille.

¹⁰ Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifiointista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus) (EUVL L 151, 7.6.2019, s. 15).

- (26) Jotta turvallisuuteen liittyviä riskejä voitaisiin jatkuvasti arvioida ja lieventää, sertifioituille eurooppalaisille digitaalisen identiteetin lompakoille olisi tehtävä säännöllisesti haavoittuvuusarvioita, joissa pyritään havaitsemaan mahdolliset haavoittuvuudet eurooppalaisen digitaalisen identiteetin lompakon sertifioituissa tuote-, prosessi- ja palvelukomponenteissa.
- (27) Tässä asetuksessa säädetyillä olennaisilla kyberturvallisuusvaatimuksilla suojataan käyttäjiä ja yrityksiä kyberturvariskeiltä, joten niillä pyritään myös osaltaan parantamaan henkilötietojen ja yksityisyyden suojaa. Kyberturvanäkökohtien standardoinnin ja sertifiointin synergioihin olisi pyrittävä yhteistyössä komission, eurooppalaisten standardointiorganisaatioiden, Euroopan unionin kyberturvallisuusviraston (ENISA), asetuksella (EU) 2016/679 perustetun Euroopan tietosuojaneuvoston ja kansallisten tietosuojaviranomaisten välillä.

- (28) Unionin kansalaisten ja unionissa asuvien henkilöiden eurooppalaisen digitaalisen identiteetin lompakon käyttösuhteen aloittamista olisi helpotettava käyttämällä sähköisen tunnistamisen menetelmiä, jotka on myönnetty korkealla varmuustasolla. Korotetulla varmuustasolla myönnettyjä sähköisen tunnistamisen menetelmiä olisi käytettävä ainoastaan, jos yhdenmukaistetut tekniset eritelmät ja menettelyt, joissa käytetään korotetulla varmuustasolla myönnettyjä sähköisen tunnistamisen menetelmiä yhdessä täydentävien henkilöllisyyden todentamismenetelmien kanssa, mahdollistavat tässä asetuksessa säädettyjen korkeaa varmuustasoa koskevien vaatimusten täyttymisen. Tällaisten täydentävien menetelmien olisi oltava luotettavia ja helppokäyttöisiä, ja ne voisivat perustua mahdollisuuteen käyttää käyttösuhteen aloittamisen etämenettelyjä, hyväksytyjä varmenteita, joita tuetaan hyväksytyillä sähköisillä allekirjoituksilla, hyväksytyjä sähköisiä attribuuttitodistuksia tai niiden yhdistelmää. Jotta voidaan varmistaa eurooppalaisten digitaalisen identiteetin lompakoiden riittävä käyttöönnotto, täytäntöönpanosäädöksissä olisi vahvistettava yhdenmukaistetut tekniset eritelmät ja menettelyt käyttäjien käyttösuhteen aloittamiseksi sähköisen tunnistamisen menetelmiä käyttäen, mukaan lukien korotetulla varmuustasolla myönnettyt menetelmät.

- (29) Tämän asetuksen tavoitteena on tarjota käyttäjälle täysin mobiili, turvallinen ja käyttäjäystävällinen eurooppalainen digitaalisen identiteetin lompakko. Eurooppalaisten digitaalisen identiteetin lompakoiden olisi siirtymätoimenpiteenä siihen saakka, kun saatavilla on sertifioituja väärinkäytöltä suojattuja ratkaisuja, kuten käyttäjien laitteissa olevia turvatekijöitä, voitava käyttää salausaineiston ja muiden arkaluonteisten tietojen suojaamiseksi sertifioituja ulkoisia turvatekijöitä tai ilmoitettuja sähköisiä tunnistamisen menetelmiä, joiden varmuustaso on korkea, osoittaakseen, että tämän asetuksen asiaankuuluvia vaatimuksia eurooppalaisen digitaalisen identiteetin lompakon varmuustason osalta noudatetaan. Tämä asetusta ei saisi rajoittaa sertifioidun ulkoisen turvatekijän myöntämistä ja käyttöä koskevien kansallisten edellytysten soveltamista, jos kyseinen siirtymätoimenpide on siitä riippuvainen.
- (30) Eurooppalaisten digitaalisen identiteetin lompakoiden olisi varmistettava julkisiin ja yksityisiin palveluihin pääsyä helpottavan tunnistamisen ja todentamisen korkein tietosuoja- ja turvallisuustaso riippumatta siitä, tallennetaanko kyseiset tiedot paikallisesti vai pilvipohjaisiin ratkaisuihin, ottaen asianmukaisesti huomioon erilaiset riskitasot.

- (31) Eurooppalaisten digitaalisen identiteetin lompakoiden turvallisuuden olisi oltava sisäänrakennettua, ja niissä olisi otettava käyttöön edistyneitä turvaominaisuuksia, jotka suojelevat identiteettivarkauksilta ja muilta tietovarkauksilta, palvelunestolta ja muilta kyberuhkilta. Tällaiseen tietoturvaan olisi sisällytettävä uusimmat salaus- ja tallennusmenetelmät, jotka ovat ainoastaan käyttäjän saatavilla ja ainoastaan hänen purettavissaan, ja jotka perustuvat päästä päähän salattuun viestintään muiden eurooppalaisten digitaalisen identiteetin lompakkojen ja luottavien osapuolten kanssa. Lisäksi eurooppalaisten digitaalisen identiteetin lompakoiden olisi edellytettävä suojattua, nimenomaista ja aktiivista käyttäjän vahvistusta eurooppalaisten digitaalisen identiteetin lompakoiden kautta suoritetuille toimille.
- (32) Eurooppalaisten digitaalisen identiteetin lompakoiden maksuton käyttö ei saisi johtaa muiden tietojen käsittelyyn kuin niiden tietojen, mitä eurooppalaisen digitaalisen identiteetin lompakon palvelujen tarjoaminen edellyttää. Tässä asetuksessa ei olisi sallittava sitä, että eurooppalaisen digitaalisen identiteetin lompakon tarjoaja käyttää eurooppalaiseen digitaalisen identiteetin lompakkoon tallennettuja tai lompakon käytön seurauksena kerättyjä henkilötietoja muihin tarkoituksiin kuin eurooppalaisen digitaalisen identiteetin lompakon palvelujen tarjoamiseen. Yksityisyyden varmistamiseksi eurooppalaisten digitaalisen identiteetin lompakon tarjoajien olisi varmistettava, että lompakon käyttöä ei voi havaita, siten, että tietoja ei kerätä eikä lompakon käyttäjien tapahtumia tarkkailla. Se, että tietoja ei voi havaita, tarkoittaa, että palveluntarjoajat eivät saa pystyä näkemään käyttäjän suorittamien tapahtumien yksityiskohtia. Erityistapauksissa eurooppalaisten digitaalisen identiteetin lompakoiden tarjoajille voitaisiin kuitenkin myöntää pääsy tietoihin, jotka ovat tarpeen jonkin tietyn eurooppalaiseen digitaalisen identiteetin lompakoihin liittyvän palvelun tarjoamiseksi, jos käyttäjä on kussakin erityistapauksessa antanut tähän nimenomaisen etukäteissuostumuksensa ja asetusta (EU) 2016/679 noudatetaan täysimääräisesti.

- (33) Eurooppalaisten digitaalisen identiteetin lompakoiden avoimuus ja niiden tarjoajien vastuuvollisuus ovat keskeisiä tekijöitä yhteiskunnallisen luottamuksen luomisessa ja kehityksen hyväksymisen edistämiseksi. Eurooppalaisten digitaalisen identiteetin lompakoiden toiminnan olisi näin ollen oltava läpinäkyvää ja sen olisi erityisesti mahdollistettava todennettavissa oleva henkilötietojen käsittely. Tätä varten jäsenvaltioiden olisi luovutettava eurooppalaisten digitaalisen identiteetin lompakoiden käyttäjäsovellusten ohjelmistokomponenttien lähdekoodi, myös sellaisten komponenttien osalta, jotka liittyvät henkilötietojen ja oikeushenkilöiden tietojen käsittelyyn. Tämän lähdekoodin julkaisemisen avoimen lähdekoodin lisenssillä tulisi antaa yhteiskunnalle, mukaan lukien käyttäjät ja kehittäjät, mahdollisuus ymmärtää lähdekoodin toiminta ja tarkistaa koodia. Tämä lisäisi käyttäjien luottamusta lompakon ekosysteemiin ja parantaisi eurooppalaisten digitaalisen identiteetin lompakoiden turvallisuutta, koska kaikki voisivat ilmoittaa koodien haavoittuvuuksista ja virheistä. Näin on tarkoitus kannustaa toimittajia toimittamaan ja ylläpitämään erittäin turvallisia tuotteita. Tietyissä tapauksissa jäsenvaltiot voisivat kuitenkin asianmukaisesti perustelluista syistä, erityisesti yleisen turvallisuuden nimissä, rajoittaa sellaisten käytettyjen kirjastojen, viestintäkanavien tai muiden sellaisten elementtien lähdekoodin julkistamista, joita ei säilytetä käyttäjän laitteessa.
- (34) Käyttäjän olisi voitava vapaasti päättää eurooppalaisen digitaalisen identiteetin lompakon käytöstä ja sen lopettamisesta. Jäsenvaltioiden olisi kehitettävä yksinkertaisia ja turvallisia menettelyjä, joiden avulla käyttäjä voi pyytää eurooppalaisen digitaalisen identiteetin lompakon voimassaolon välitöntä peruuttamista esimerkiksi katoamis- tai varkaustapauksissa. Sellaisia tapauksia varten, joissa käyttäjä kuolee tai oikeushenkilön toiminta lakkaa, olisi perustettava mekanismi, jonka avulla luonnollisen henkilön pesänselvityksestä tai oikeushenkilön omaisuuden selvittämisestä vastaava viranomainen voi pyytää eurooppalaisten digitaalisen identiteetin lompakkojen välitöntä peruuttamista.

- (35) Jotta edistettäisiin eurooppalaisten digitaalisen identiteetin lompakkojen käyttöönottoa ja digitaalisten identiteettien laajempaa käyttöä, jäsenvaltioiden olisi edistettävä asiaankuuluvien palvelujen etuja, ja sen lisäksi niiden olisi yhteistyössä yksityisen sektorin, tutkijoiden ja tiedemaailman kanssa kehitettävä koulutusohjelmia, joilla pyritään vahvistamaan jäsenvaltioiden kansalaisten ja asukkaiden, erityisesti muita heikommassa asemassa olevien ryhmien, kuten vammaisten henkilöiden ja ikääntyneiden henkilöiden, digitaalisia taitoja. Jäsenvaltioiden olisi myös lisättävä tiedotuskampanjoiden avulla tietoisuutta eurooppalaisen digitaalisen identiteetin lompakon hyödyistä ja riskeistä.
- (36) Sen varmistamiseksi, että eurooppalainen digitaalisen identiteetin kehys on avoin innovoinnille ja tekniikan kehitykselle ja pystyy mukautumaan tulevaisuuden vaatimuksiin, jäsenvaltioita kannustetaan perustamaan yhdessä testausympäristöjä innovatiivisten ratkaisujen testaamiseksi valvotussa ja turvallisessa ympäristössä, jotta voidaan erityisesti parantaa ratkaisujen toimivuutta, turvallisuutta ja yhteentoimivuutta ja niiden tarjoamaa henkilötietojen suojaa sekä vaikuttaa teknisten viitetietojen ja oikeudellisten vaatimusten tuleviin päivityksiin. Tämän ympäristön olisi edistettävä pk-yritysten, startup-yritysten, yksittäisten innovoijien ja tutkijoiden sekä asiaankuuluvien toimialan sidosryhmien osallisuutta. Tällaisten aloitteiden on tarkoitus edistää ja vahvistaa unionin kansalaisille ja unionin muille asukkaille tarjottavien eurooppalaisten digitaalisen identiteetin lompakoiden vaatimustenmukaisuutta ja teknistä vakautta ja estää siten sellaisten ratkaisujen kehittäminen, jotka eivät ole unionin tietosuojalainsäädännön mukaisia tai joissa on tietoturvariskejä.

- (37) Euroopan parlamentin ja neuvoston asetuksella (EU) 2019/1157¹¹ lisättiin henkilökorttien turvallisuutta parannetuilla turvaominaisuuksilla elokuuhun 2021 mennessä. Jäsenvaltioiden olisi harkittava mahdollisuutta ilmoittaa näistä turvaominaisuuksista sähköisen tunnistamisen järjestelmien yhteydessä sähköisen tunnistamisen menetelmien rajatylittävän saatavuuden laajentamiseksi.
- (38) Sähköisen tunnistamisen järjestelmien ilmoitusmenettelyä olisi yksinkertaistettava ja nopeutettava, jotta voidaan edistää helppokäyttöisten, luotettavien, turvallisten ja innovatiivisten todentamis- ja tunnistusratkaisujen saatavuutta ja tarvittaessa kannustaa yksityisiä tunnistustietojen tarjoajia tarjoamaan sähköisen tunnistamisen järjestelmiä jäsenvaltioiden viranomaisille, jotta niistä voidaan ilmoittaa asetuksen (EU) N:o 910/2014 mukaisina kansallisina sähköisen tunnistamisen järjestelminä.
- (39) Nykyisten ilmoitus- ja vertaisarviointimenettelyjen virtaviivaistaminen estää erilaisten ilmoitettujen sähköisen tunnistamisen järjestelmien arvioinnin epäyhtenäiset mallit ja helpottaa luottamuksen rakentamista jäsenvaltioiden välillä. Uusien yksinkertaisempien mekanismien on tarkoitus edistää jäsenvaltioiden yhteistyötä niiden ilmoittamien sähköisen tunnistamisen järjestelmien turvallisuuden ja yhteentoimivuuden alalla.
- (40) Jäsenvaltiot hyötyvät uusista joustavista välineistä, joilla varmistetaan tämän asetuksen ja sen mukaisesti annettujen asiaa koskevien täytäntöönpanosäädösten vaatimusten noudattaminen. Tämän asetuksen on tarkoitus antaa jäsenvaltioille mahdollisuus käyttää akkreditoitujen vaatimustenmukaisuuden arviointilaitosten tekemiä raportteja ja arviointeja, kuten asetuksen (EU) 2019/881 nojalla unionin tasolla perustettavien sertifiointijärjestelmien yhteydessä edellytetään, tukeakseen väitteitään siitä, että järjestelmät tai niiden osat ovat asetuksen (EU) N:o 910/2014 mukaisia.

¹¹ Euroopan parlamentin ja neuvoston asetus (EU) 2019/1157, annettu 20 päivänä kesäkuuta 2019, unionin kansalaisten henkilökorttien sekä oikeuttaan vapaaseen liikkuvuuteen käyttäville unionin kansalaisille ja heidän perheenjäsenilleen myönnettävien oleskeluasiakirjojen turvallisuuden lisäämisestä (EUVL L 188, 12.7.2019, s. 67).

- (41) Julkiset palveluntarjoajat käyttävät henkilöiden tunnistetietoja, jotka ovat saatavilla asetuksen (EU) N:o 910/2014 mukaisissa sähköisen tunnistamisen menetelmissä yhdistääkseen toisesta jäsenvaltiosta tulevien käyttäjien sähköisen identiteetin niihin tunnistetietoihin, jotka heille on annettu rajatylittävää henkilöllisyyden linkittämistä suorittavassa jäsenvaltiossa. Ilmoitettujen sähköisen tunnistamisen järjestelmien mukaisten vähimmäistietokokonaisuuksien käytöstä huolimatta henkilöllisyyden tarkan linkittämisen varmistaminen silloin, kun jäsenvaltiot toimivat luottavina osapuolina, edellyttää kuitenkin monissa tapauksissa lisätietoja käyttäjästä ja erityisiä täydentäviä yksilöllisiä tunnistusmenettelyjä, jotka on toteutettava kansallisella tasolla. Jotta voidaan edelleen tukea sähköisen tunnistamisen menetelmien käytettävyyttä, tarjota parempia julkisia verkkopalveluja ja lisätä käyttäjien sähköistä henkilöllisyyttä koskevaa oikeusvarmuutta, asetuksessa (EU) N:o 910/2014 olisi edellytettävä, että jäsenvaltiot toteuttavat erityisiä verkkotoimenpiteitä yksiselitteisen henkilöllisyyden linkittämisen varmistamiseksi, kun käyttäjät aikovat käyttää verkossa olevia rajatylittäviä julkisia palveluja.
- (42) Eurooppalaisia digitaalisen identiteetin lompakoita kehitettäessä on olennaisen tärkeää ottaa huomioon käyttäjien tarpeet. Saatavilla olisi oltava mielekkäitä käyttötapauksia ja verkkopalveluja, jotka perustuvat eurooppalaiseen digitaalisen identiteetin lompakoihin. Käyttömukavuuden lisäämiseksi ja tällaisten palvelujen rajatylittävän saatavuuden varmistamiseksi on tärkeää toteuttaa toimia, joilla edistetään samanlaista lähestymistapaa verkkopalvelujen suunnitteluun, kehittämiseen ja toteuttamiseen kaikissa jäsenvaltioissa. Eurooppalaiseen digitaalisen identiteetin lompakoihin perustuvien verkkopalvelujen suunnittelua, kehittämistä ja toteuttamista koskevista ei-sitovista suuntaviivoista voi tulla hyödyllinen väline tämän tavoitteen saavuttamiseksi. Näitä suuntaviivoja laadittaessa olisi otettava asianmukaisesti huomioon unionin yhteentoimivuuskehys. Jäsenvaltioilla olisi oltava johtava rooli niiden hyväksymisessä.

- (43) Euroopan parlamentin ja neuvoston direktiivin (EU) 2019/882¹² mukaisesti vammaisten henkilöiden olisi voitava käyttää eurooppalaisia digitaalisen identiteetin lompakkoja, luottamuspalveluja ja niiden tarjoamiseksi tarvittavia loppukäyttäjätuotteita tasavertaisesti muiden käyttäjien kanssa.
- (44) Tämän asetuksen tehokkaan täytäntöönpanon varmistamiseksi olisi vahvistettava sekä hyväksytyjen että ei-hyväksytyjen luottamuspalvelujen tarjoajien hallinnollisten sakkojen enimmäismäärän vähimmäismäärä. Jäsenvaltioiden olisi säädettävä tehokkaista, oikeasuhteisista ja varoittavista seuraamuksista. Seuraamuksia määritettäessä olisi otettava asianmukaisesti huomioon asianomaisten yhteisöjen koko, niiden liiketoimintamallit ja rikkomusten vakavuus.
- (45) Jäsenvaltioiden olisi vahvistettava säännöt, jotka koskevat seuraamuksia rikkomuksista, kuten suorista tai epäsuorista käytännöistä, jotka johtavat sekaannukseen ei-hyväksytyjen ja hyväksytyjen luottamuspalvelujen välillä tai siihen, että ei-hyväksytyt luottamuspalvelun tarjoajat käyttävät EU:n luotettavuusmerkkiä väärin. EU:n luotettavuusmerkkiä ei saisi käyttää tavoin, jotka suoraan tai välillisesti johtavat käsitykseen, jonka mukaan kyseisten palveluntarjoajien tarjoamat ei-hyväksytyt luottamuspalvelut olisivat hyväksytyjä.
- (46) Tämän asetuksen ei olisi katettava näkökohtia, jotka liittyvät sellaisten sopimusten tai muiden oikeudellisten velvoitteiden vahvistamiseen ja pätevyYTEEN, joihin sisältyy unionin oikeudessa tai kansallisessa lainsäädännössä säädettyjä muotovaatimuksia. Sen ei saisi myöskään vaikuttaa kansallisiin muotovaatimuksiin, jotka koskevat julkisia rekistereitä, erityisesti kauppa- ja kiinteistörekistereitä.

¹² Euroopan parlamentin ja neuvoston direktiivi (EU) 2019/882, annettu 17 päivänä huhtikuuta 2019, tuotteiden ja palvelujen esteettömyysvaatimuksista (EUVL L 151, 7.6.2019, s. 70).

(47) Luottamuspalvelujen tarjoamisesta ja käytöstä sekä niiden tarjoamasta käyttömukavuudesta ja oikeusvarmuudesta rajatylittävien liiketoimien yhteydessä erityisesti silloin, kun käytetään hyväksytyjä luottamuspalveluja, on tulossa yhä tärkeämpää kansainväliselle kaupalle ja yhteistyölle. Unionin kansainväliset kumppanit ovat luomassa luottamuskehyskiä, jotka ovat saaneet innoituksensa asetuksesta (EU) N:o 910/2014. Hyväksytyjen luottamuspalvelujen ja niiden tarjoajien tunnustamisen helpottamiseksi komissio voi hyväksyä täytäntöönpanosäädöksiä sellaisten edellytysten vahvistamiseksi, joiden täytyessä kolmansien maiden luottamuskehysten voidaan katsoa vastaavan tässä asetuksessa säädettyä hyväksytyjä luottamuspalveluja ja niiden tarjoajia koskevaa kehystä. Tällaisella lähestymistavalla täydennettäisiin mahdollisuutta unioniin ja kolmansiin maihin sijoittautuneiden luottamuspalvelujen ja niiden tarjoajien vastavuoroiseen tunnustamiseen Euroopan unionin toiminnasta tehdyn sopimuksen 218 artiklan mukaisesti. Vahvistettaessa edellytyksiä, joiden täytyessä kolmansien maiden luottamuskehysten voitaisiin katsoa vastaavan asetuksessa (EU) N:o 910/2014 säädettyä hyväksytyjen luottamuspalvelujen ja niiden tarjoajien luottamuskehystä, olisi varmistettava Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2555¹³ ja asetuksen (EU) 2016/679 asiaankuuluvien säännösten noudattaminen sekä luotettujen luetteloiden käyttö oleellisena tekijänä luottamuksen rakentamisessa.

¹³ Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi) (EUVL L 333, 27.12.2022, s. 80).

- (48) Tämän asetuksen on tarkoitus edistää valinnanvaraa ja mahdollisuutta vaihdella eurooppalaisten digitaalisten identiteetin lompakoiden välillä, jos jäsenvaltio on hyväksynyt useamman kuin yhden eurooppalaisen digitaalisen identiteetin lompakon ratkaisun alueellaan. Jotta vältetään lukkiutumisvaikutukset tällaisissa tilanteissa, jos se on teknisesti mahdollista, eurooppalaisten digitaalisen identiteetin lompakoiden tarjoajien olisi varmistettava tietojen tosiasiallinen siirrettävyys eurooppalaisen digitaalisen identiteetin lompakon käyttäjän pyynnöstä, eikä niiden olisi voitava käyttää sopimusperusteisia, taloudellisia tai teknisiä esteitä ehkäistäkseen sujuvan siirtymisen yhdestä eurooppalaisen digitaalisen identiteetin lompakosta toiseen eikä tehdä ajatusta siirtymisestä liian vaikeaksi.
- (49) Eurooppalaisten digitaalisen identiteetin lompakoiden asianmukaisen toiminnan varmistamiseksi eurooppalaisten digitaalisen identiteetin lompakoiden tarjoajat tarvitsevat tehokkaan yhteentoimivuuden sekä oikeudenmukaiset, kohtuulliset ja syrjimättömät ehdot, jotta eurooppalaiset digitaalisen identiteetin lompakot voivat käyttää mobiililaitteiden tiettyjä laitteisto- ja ohjelmisto-ominaisuuksia. Näihin komponentteihin voisi kuulua erityisesti lähitiedonsiirron antenneja ja suojattuja elementtejä, mukaan lukien UICC-kortit, sulautetut turvaelementit, mikroSD-kortit ja Bluetooth Low Energy - tekniikka. Näiden komponenttien käyttömahdollisuus voisi olla matkaviestinoperaattoreiden ja laitevalmistajien valvonnassa. Sen vuoksi mobiililaitteiden alkuperäiset laitevalmistajat tai sähköisten viestintäpalvelujen tarjoajat eivät saisi evätä pääsyä tällaisiin komponentteihin, jos se on tarpeen eurooppalaisten digitaalisen identiteetin lompakoiden palvelujen tarjoamiseksi. Lisäksi yrityksiin, jotka on nimetty ydinalustapalvelujen portinvartijoiksi ja jotka komissio on sisällyttänyt Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/1925¹⁴ mukaiseen luetteloon, olisi edelleen sovellettava mainitun asetuksen erityissäännöksiä, jotka perustuvat sen 6 artiklan 7 kohtaan.

¹⁴ Euroopan parlamentin ja neuvoston asetukset (EU) 2022/1925, annettu 14 päivänä syyskuuta 2022, kilpailullisista ja oikeudenmukaisista markkinoista digitaalisella ja digitaalialalla ja direktiivien (EU) 2019/1937 ja (EU) 2020/1828 muuttamisesta (digimarkkinasäädös) (EUVL L 265, 12.10.2022, s. 1).

(50) Jotta voidaan virtaviivaistaa luottamuspalvelun tarjoajille asetettuja kyberturvallisuusvelvoitteita ja antaa näille palveluntarjoajille ja niistä vastaaville toimivaltaisille viranomaisille mahdollisuus hyötyä direktiivillä (EU) 2022/2555 vahvistetusta oikeudellisesta kehyksestä, luottamuspalvelujen edellytetään toteutettavan kyseisen direktiivin mukaiset asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten toimenpiteet, joilla puututaan järjestelmän toimintahäiriöihin, inhimillisiin virheisiin, vihamielisiin toimiin tai luonnonilmiöihin, jotta voidaan hallita niiden verkko- ja tietojärjestelmien turvallisuuteen kohdistuvia riskejä, joita kyseiset palveluntarjoajat käyttävät palvelujensa tarjoamisessa, sekä ilmoittaa merkittävistä poikkeamista ja kyberuhkista kyseisen direktiivin mukaisesti. Poikkeamista ilmoittamisen osalta luottamuspalvelun tarjoajien olisi ilmoitettava kaikista poikkeamista, joilla on merkittävä vaikutus niiden palvelujen tarjoamiseen, mukaan lukien häiriöt, jotka johtuvat laitteiden varastamisesta tai katoamisesta, verkkokaapeleille aiheutuneista vahingoista tai henkilöiden tunnistamisen yhteydessä tapahtuneista turvapoikkeamista. Direktiivin (EU) 2022/2555 mukaisten kyberturvallisuusriskien hallintaa koskevien vaatimusten ja raportointivelvoitteiden olisi katsottava täydentävän tämän asetuksen nojalla luottamuspalvelujen tarjoajille asetettuja vaatimuksia. Direktiivin (EU) 2022/2555 mukaisesti nimettyjen toimivaltaisten viranomaisten olisi tarvittaessa sovellettava edelleen vakiintuneita kansallisia käytäntöjä tai ohjeita, jotka liittyvät turvallisuus- ja raportointivaatimusten täytäntöönpanoon ja tällaisten vaatimusten noudattamisen valvontaan asetuksen (EU) N:o 910/2014 mukaisesti. Tämä asetus ei vaikuta velvoitteeseen ilmoittaa henkilötietojen tietoturvaloukkauksista asetuksen (EU) 2016/679 nojalla.

- (51) Olisi kiinnitettävä asianmukaista huomiota tehokkaan yhteistyön varmistamiseen asetuksen (EU) N:o 910/2014 46 b artiklan nojalla nimettyjen valvontaelinten ja direktiivin (EU) 2022/2555 8 artiklan 1 kohdan nojalla nimettyjen tai perustettujen toimivaltaisten viranomaisten välillä. Jos kyseinen valvontaelin on muu kuin kyseinen toimivaltainen viranomainen, niiden olisi tehtävä tiivistä ja oikea-aikaista yhteistyötä vaihtamalla asiaankuuluvia tietoja, jotta voidaan varmistaa tehokas valvonta ja se, että luottamuspalvelun tarjoajat noudattavat asetuksessa (EU) N:o 910/2014 ja direktiivissä (EU) 2022/2555 säädettyjä vaatimuksia. Asetuksen (EU) N:o 910/2014 nojalla nimetyillä valvontaelimillä olisi erityisesti oltava oikeus pyytää direktiivin (EU) 2022/2555 nojalla nimettyjä tai perustettuja toimivaltaisia viranomaisia antamaan hyväksytyn aseman myöntämiseksi tarvittavat tiedot ja toteuttamaan valvontatoimia sen varmistamiseksi, että luottamuspalvelun tarjoajat noudattavat direktiivin (EU) 2022/2555 mukaisia asiaankuuluvia vaatimuksia, tai vaatimaan niitä korjaamaan vaatimusten noudattamatta jättämisen.

- (52) On olennaisen tärkeää säätää oikeudellisesta kehyksestä, jolla edistetään rajat ylittävää tunnustamista sähköisiin rekisteröityihin jakelupalveluihin liittyvien olemassa olevien kansallisten oikeusjärjestelmien välillä. Tämä kehys voisi myös avata unionin luottamuspalvelun tarjoajille uusia markkinamahdollisuuksia uusien unionin laajuisten sähköisten rekisteröityjen jakelupalvelujen tarjoamiseksi. Sen varmistamiseksi, että hyväksytyä sähköistä rekisteröityä jakelupalvelua käytettäessä tiedot toimitetaan oikealle vastaanottajalle, hyväksytyjen sähköisten rekisteröityjen jakelupalvelujen olisi varmistettava täysin varmasti vastaanottajan tunnistaminen, kun taas lähettäjän tunnistamiseen riittää korkea luottamustaso. Jäsenvaltioiden olisi kannustettava hyväksytyjen sähköisten rekisteröityjen jakelupalvelujen tarjoajia varmistamaan, että niiden palvelut ovat yhteentoimivia muiden hyväksytyjen luottamuspalvelun tarjoajien tarjoamien hyväksytyjen sähköisten rekisteröityjen jakelupalvelujen kanssa, jotta sähköisesti rekisteröidyt tiedot voidaan siirtää helposti kahden tai useamman hyväksytyyn luottamuspalvelun tarjoajan välillä ja jotta oikeudenmukaisia käytäntöjä voidaan edistää sisämarkkinoilla.
- (53) Useimmissa tapauksissa unionin kansalaiset ja muut asukkaat eivät voi vaihtaa valtioiden rajojen yli turvallisesti ja korkeatasoisella tietosuojatasolla henkilöllisyyteensä liittyviä digitaalisia tietoja, kuten osoitetta, ikää, ammattipätevyyttä, ajokorttia ja muita lupia sekä maksutietoja.
- (54) Olisi oltava mahdollista antaa ja käsitellä luotettavia sähköisiä attribuutteja ja auttaa vähentämään hallinnollista taakkaa antamalla unionin kansalaisille ja muille asukkaille mahdollisuus käyttää niitä yksityisissä ja julkisissa transaktioissaan. Unionin kansalaisten ja muiden asukkaiden olisi esimerkiksi voitava osoittaa, että heillä on hallussaan jonkin jäsenvaltion viranomaisen myöntämä voimassa oleva ajokortti, jonka muiden jäsenvaltioiden asianomaiset viranomaiset voivat todentaa ja johon ne voivat luottaa, tai käyttää sosiaaliturvaan liitettyjä tietojaan tai tulevia sähköisiä matkustusasiakirjoja rajatylittävässä yhteydessä.

- (55) Palveluntarjoaja, joka myöntää sähköisessä muodossa olevia todistettuja attribuutteja, kuten tutkintotodistuksia, lisensejä, syntymätodistuksia tai valtuuksia ja valtuutuksia edustaa luonnollisia henkilöitä tai oikeushenkilöitä tai toimia heidän taikka niiden puolesta, olisi pidettävä luottamuspalvelun tarjoajana, joka myöntää sähköisiä attribuuttitodistuksia. Sähköisen attribuuttitodistuksen oikeusvaikutuksia ei saisi kieltää sillä perusteella, että se on sähköisessä muodossa tai että se ei täytä hyväksytyyn sähköisen attribuuttitodistuksen vaatimuksia. Olisi vahvistettava yleiset vaatimukset sen varmistamiseksi, että hyväksytyllä sähköisellä attribuuttitodistuksella on samanlaiset oikeusvaikutukset kuin laillisesti annetuilla paperimuotoisilla todistuksilla. Näitä vaatimuksia olisi kuitenkin sovellettava rajoittamatta sellaisen unionin oikeuden tai kansallisen lainsäädännön soveltamista, jossa määritellään muotoa koskevia alakohtaisia lisävaatimuksia, joilla on oikeusvaikutuksia, ja tarvittaessa erityisesti rajoittamatta hyväksytyyn sähköisen attribuuttitodistuksen rajatylittävää tunnustamista.
- (56) Eurooppalaisten digitaalisen identiteetin lompakoiden laajan saatavuuden ja käytettävyyden olisi lisättävä niiden hyväksyntää ja niihin kohdistuvaa luottamusta sekä yksityishenkilöiden että yksityisten palveluntarjoajien keskuudessa. Tästä syystä yksityisten luottavien osapuolten, jotka tarjoavat palveluja esimerkiksi liikenteen, energian, pankki- ja rahoituspalvelujen, sosiaaliturvan, terveydenhuollon, juomaveden, postipalvelujen, digitaalisen infrastruktuurin, televiestinnän tai koulutuksen aloilla, olisi hyväksyttävä eurooppalaisten digitaalisen identiteetin lompakoiden käyttö sellaisten palvelujen tarjoamisessa, joissa unionin oikeuden tai kansallisen lainsäädännön tai sopimusvelvoitteiden mukaisesti edellytetään käyttäjien vahvaa todentamista verkossa tapahtuvaa tunnistamista varten. Luottavan osapuolen eurooppalaisen digitaalisen identiteetin lompakon käyttäjälle tekemien tietopyyntöjen olisi oltava tarpeellisia ja oikeassa suhteessa aiottuun käyttöön tietystä tapauksessa, niiden olisi oltava tietojen minimoinnin periaatteen mukaisia ja niiden olisi varmistettava avoimuus sen suhteen, mitä tietoja jaetaan ja mihin tarkoituksiin. Eurooppalaisen digitaalisen identiteetin lompakon käytön ja hyväksymisen helpottamiseksi sen käyttöönotossa olisi otettava huomioon toimialan laajalti hyväksytyt standardit ja eritelvät.

- (57) Jos Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2065¹⁵ 33 artiklan 1 kohdassa määritellyt erittäin suuret verkkoalustat vaativat käyttäjien todentautuvan verkkopalveluihin pääsyä varten, kyseiset alustat olisi velvoitettava hyväksymään eurooppalaisten digitaalisen identiteetin lompakoiden käyttö käyttäjän vapaaehtoisesta pyynnöstä. Käyttäjillä ei saisi olla velvollisuutta käyttää eurooppalaista digitaalisen identiteetin lompakkoa yksityisten palvelujen saamiseksi, eikä heidän pääsyään palveluihin saisi rajoittaa tai estää sillä perusteella, että he eivät käytä eurooppalaista digitaalisen identiteetin lompakkoa. Jos käyttäjät kuitenkin niin haluavat, erittäin suurten verkkoalustojen olisi hyväksyttävä ne tähän tarkoitukseen noudattaen tietojen minimoinnin periaatetta ja käyttäjien oikeutta käyttää vapaasti valittuja pseudonyymejä. Velvoite hyväksyä eurooppalainen digitaalisen identiteetin lompakko on tarpeen, jotta voidaan paremmin suojata käyttäjiä petoksilta ja varmistaa korkeatasoinen tietosuojaa, kun otetaan huomioon erittäin suurten verkkoalustojen merkitys, mikä johtuu niiden kattavuudesta, erityisesti palvelun käyttäjien ja taloudellisten transaktioiden lukumääränä ilmaistuna.
- (58) Unionin tasolla olisi kehitettävä käytäntösääntöjä, jotta edistettäisiin sähköisen tunnistamisen menetelmien, myös eurooppalaisten digitaalisen identiteetin lompakoiden, laajaa saatavuutta ja käytettävyyttä tämän asetuksen soveltamisalalla. Käytännössä olisi helpotettava sitä, että palveluntarjoajat, joita ei voida pitää erittäin suurina verkkoalustoina ja jotka käyttävät kolmannen osapuolen tarjoamia sähköisiä tunnistuspalveluja käyttäjien todentamisessa, hyväksyvät laajasti sähköisen tunnistamisen menetelmät, myös eurooppalaiset digitaalisen identiteetin lompakot.

¹⁵ Euroopan parlamentin ja neuvoston asetus (EU) 2022/2065, annettu 19 päivänä lokakuuta 2022, digitaalisten palvelujen sisämarkkinoista ja direktiivin 2000/31/EY muuttamisesta (digipalvelusäädös) (EUVL L 277, 27.10.2022, s. 1).

- (59) Valikoiva luovuttaminen tarkoittaa, että tietojen omistajalle annetaan valtuudet luovuttaa vain tietyt laajemman tietokokonaisuuden osat, jotta vastaanottava yhteisö saa ainoastaan käyttäjän pyytämän palvelun tarjoamiseen tarvittavat tiedot. Eurooppalaisen digitaalisen identiteetin lompakon olisi teknisesti mahdollistettava attribuuttien valikoiva luovuttaminen luottaville osapuolille. Käyttäjälle olisi oltava teknisesti mahdollista valikoivasti luovuttaa attribuutit, myös useista erillisistä sähköisistä todistuksista, ja yhdistää ja esittää ne saumattomasti luottaville osapuolille. Tästä ominaisuudesta olisi tultava eurooppalaisen digitaalisen identiteetin lompakon perusominaisuus, mikä lisää käyttömukavuutta ja henkilötietojen suojausta, johon kuuluu tietojen minimointi.
- (60) Ellei unionin oikeuden tai kansallisen lainsäädännön erityisissä säännöissä edellytetä, että käyttäjät tunnistautuvat, palvelujen käyttöä pseudonyymillä ei saisi kieltää.

- (61) Hyväksytyjen luottamuspalvelun tarjoajien osana hyväksytyä sähköistä attribuuttitodistusta tarjoamat attribuutit olisi tarkastettava virallisista lähteistä joko suoraan hyväksytyyn luottamuspalvelun tarjoajan toimesta tai sellaisten nimettyjen välittäjien avulla, jotka on unionin oikeuden tai kansallisen lainsäädännön mukaisesti tunnustettu kansallisella tasolla harjoittamaan todistettujen attribuuttien suojattua vaihtoa tunnistuspalvelun tai attribuuttitodistusten tarjoajien ja luottavien osapuolten välillä. Jäsenvaltioiden olisi otettava käyttöön asianmukaiset kansallisen tason mekanismit sen varmistamiseksi, että hyväksytyjä sähköisiä attribuuttitodistuksia myöntävät hyväksytyt luottamuspalvelun tarjoajat voivat sen henkilön suostumuksella, jolle todistus on myönnetty, todentaa attribuuttien aitouden virallisten lähteiden perusteella. Asianmukaisiin mekanismeihin olisi voitava kuulua erityisten välittäjien tai teknisten ratkaisujen käyttö kansallisen lainsäädännön mukaisesti, mahdollistaen virallisten lähteiden saatavuuden. Varmistamalla, että saatavilla on attribuuttien todentamisen virallisista lähteistä mahdollistava mekanismi, on tarkoitus helpottaa hyväksytyjen sähköisten attribuuttitodistusten hyväksytyjen luottamuspalvelujen tarjoajien asetuksessa (EU) N:o 910/2014 säädettyjen velvoitteiden noudattamista. Kyseisen asetuksen uudessa liitteessä olisi oltava luettelo attribuuttiluokista, joiden osalta jäsenvaltioiden olisi varmistettava, että toteutetaan toimenpiteitä, jotta sähköisten attribuuttitodistusten hyväksytyt tarjoajat voivat käyttäjän pyynnöstä tarkistaa sähköisesti niiden aitouden asianomaisesta virallisesta lähteestä.

- (62) Turvallisessa sähköisessä tunnistamisessa ja attribuuttitodistusten antamisessa olisi tarjottava rahoituspalvelualalle lisäjoustoa ja -ratkaisuja, jotka mahdollistavat asiakkaiden tunnistamisen ja sellaisten erityisten attribuuttien vaihdon, joita tarvitaan esimerkiksi tulevan, rahanpesutorjuntaviranomaisen perustamista koskevan asetuksen [viite lisätään ehdotuksen hyväksymisen jälkeen] mukaisten asiakkaan tuntemisvelvollisuutta koskevien vaatimusten ja sijoittajansuojalainsäädännöstä johtuvien soveltuvuusvaatimusten noudattamiseksi tai sähköisenä tunnistamisena tehtävää asiakkaan vahvaa todentamista koskevien vaatimusten noudattamisen tukemiseksi tilille kirjautumista ja maksutapahtumien käynnistämistä varten maksupalvelujen alalla.
- (63) Sähköisen allekirjoituksen oikeusvaikutuksia ei saa kiistää sillä perusteella, että se on sähköisessä muodossa tai että se ei täytä hyväksytyt sähköisen allekirjoituksen vaatimuksia. Sähköisten allekirjoitusten oikeusvaikutukset määritellään kuitenkin kansallisessa lainsäädännössä, lukuun ottamatta tässä asetuksessa säädettyjä vaatimuksia, joiden mukaan hyväksytyt sähköisen allekirjoituksen oikeusvaikutukset on katsottava samanveroisiksi kuin käsin kirjoitetun allekirjoituksen oikeusvaikutukset. Määrittäessään sähköisten allekirjoitusten oikeusvaikutuksia jäsenvaltioiden olisi otettava huomioon suhteellisuusperiaate allekirjoitettavan asiakirjan oikeudellisen arvon sekä sähköisen allekirjoituksen edellyttämän turvallisuustason ja kustannusten välillä. Sähköisten allekirjoitusten saatavuuden ja käytön lisäämiseksi jäsenvaltioita kannustetaan harkitsemaan kehittyneiden sähköisten allekirjoitusten käyttöä päivittäisissä transaktioissa, joille ne takaavat riittävän turvallisuuden ja luotettavuuden tason.

- (64) Jotta voidaan varmistaa sertifiointikäytäntöjen johdonmukaisuus kaikkialla unionissa, komission olisi annettava ohjeet hyväksytyjen sähköisen allekirjoituksen luontivälineiden ja hyväksytyjen sähköisen leiman luontivälineiden sertifiointista ja uudelleensertifiointista, mukaan lukien niiden voimassaolo ja ajalliset rajoitukset. Tämä asetus ei estä julkisia tai yksityisiä elimiä, joilla on sertifioituja hyväksytyjä sähköisen allekirjoituksen luontivälineitä, uudelleensertifioimasta väliaikaisesti tällaisia välineitä lyhyeksi sertifiointijaksoksi edellisen sertifiointimenettelyn tulosten perusteella, jos tällaista uudelleensertifiointia ei voida suorittaa laissa määritellyssä määräajassa muusta syystä kuin tietoturvaloukkauksesta tai turvallisuushäiriöstä johtuen, sanotun kuitenkin rajoittamatta velvoitetta suorittaa haavoittuvuusarviointi ja rajoittamatta sovellettavaa sertifiointikäytäntöä.

- (65) Verkkosivustojen todentamisen varmenteiden myöntämisen on tarkoitus tarjota käyttäjille korkean varmuustason takeet verkkosivuston taustalla olevan tahon identiteetistä, riippumatta siitä, mitä alustaa kyseisen identiteetin näyttämiseen käytetään. Kyseisten varmenteiden olisi lisättävä luottamusta verkossa asiointiin, koska käyttäjät luottaisivat verkkosivustoon, joka on todennettu. Tällaisten varmenteiden käytön olisi oltava vapaaehtoista verkkosivustoille. Jotta verkkosivustojen todentamisesta tulisi keino lisätä luottamusta, parantaa käyttäjän kokemusta ja edistää kasvua sisämarkkinoilla, tässä asetuksessa säädetään luottamuskehiksestä, joka sisältää tietoturvaa ja vastuuta koskevat vähimmäisvelvoitteet hyväksytyjen verkkosivustojen todentamisen varmenteiden tarjoajien ja kyseisten varmenteiden myöntämisen edellytysten osalta. Kansallisissa luotetuissa luetteloissa olisi vahvistettava verkkosivustojen todentamispalvelujen ja niiden luottamuspalvelun tarjoajien hyväksytyt asema, mukaan lukien se, että ne noudattavat kaikilta osin tämän asetuksen vaatimuksia verkkosivustojen todentamisen hyväksytyjen varmenteiden myöntämisen osalta. Verkkosivustojen todentamisen hyväksytyjen varmenteiden tunnustamisella tarkoitetaan, että verkkoselainten tarjoajat eivät saisi kieltää verkkosivustojen todentamisen hyväksytyjen varmenteiden aitoutta ainoastaan verkkosivuston verkkotunnuksen ja sen luonnollisen henkilön tai oikeushenkilön, jolle varmenne on myönnetty, välisen yhteyden todistamiseksi tai kyseisen henkilön henkilöllisyyden vahvistamiseksi. Verkkoselainten tarjoajien olisi esitettävä varmennetut henkilöllisyystiedot ja muut todistetut attribuutit loppukäyttäjälle käyttäjäystävällisellä tavalla selainympäristössä käyttämällä valitsemiaan teknisiä keinoja.

Tätä varten verkkoselainten tarjoajien olisi varmistettava tuki verkkosivustojen todentamisen hyväksytyille varmenteille, jotka on myönnetty noudattaen kaikilta osin tätä asetusta, ja yhteentoimivuus niiden kanssa. Verkkosivustojen todentamisen hyväksytyjen varmenteiden tunnustamista, yhteentoimivuutta ja tukemista koskeva velvoite ei vaikuta verkkoselainten tarjoajien vapautteen varmistaa verkkoturvaluottamus, verkkotunnusten todentaminen ja verkkoliikenteen salaus tarkoituksenmukaisimmaksi katsomallaan tavalla ja teknologialla. Jotta voidaan edistää loppukäyttäjien verkkoturvaluottamusta, verkkoselainten tarjoajien olisi poikkeuksellisissa olosuhteissa voitava toteuttaa tarpeellisia ja oikeasuhteisia varotoimenpiteitä vastauksena perusteltuihin huolenaiheisiin, jotka koskevat tietoturvaloukkauksia tai yksilöidyn varmenteen tai varmennesarjan eheyden menetystä. Kun verkkoselainten tarjoajat toteuttavat tällaisia varotoimenpiteitä, niiden olisi ilmoitettava ilman aiheetonta viivytystä komissiolle, kansalliselle valvontaelimelle, taholle, jolle todistus on myönnetty, ja kyseisen varmenteen tai varmennesarjan myöntäneelle hyväksytylle luottamuspalvelun tarjoajalle tällaista tietoturvaloukkausta tai eheyden menetystä koskevasta huolenaiheesta sekä toimenpiteistä, jotka on toteutettu kyseisen varmenteen tai varmennesarjan osalta. Nämä toimenpiteet eivät saisi rajoittaa verkkoselainten tarjoajien velvollisuutta tunnustaa verkkosivustojen todentamisen hyväksytyt varmenteet kansallisten luotettujen luetteloiden mukaisesti. Unionin kansalaisten sekä unionissa asuvien henkilöiden suojelun ja verkkosivustojen todentamisen hyväksytyjen varmenteiden käytön edistämiseksi edelleen jäsenvaltioiden viranomaisten olisi harkittava verkkosivustojen todentamisen hyväksytyjen varmenteiden sisällyttämistä verkkosivustoihinsa. Tässä asetuksessa säädetyillä toimenpiteillä, joilla pyritään lisäämään johdonmukaisuutta valvontamenettelyihin liittyvien jäsenvaltioiden erilaisten lähestymistapojen ja käytäntöjen välillä, pyritään parantamaan luottamusta verkkosivustojen todentamisen hyväksytyjen varmenteiden turvallisuuteen, laatuun ja saatavuuteen.

(66) Monet jäsenvaltiot ovat ottaneet käyttöön kansallisia vaatimuksia turvallista ja luotettavaa sähköistä arkistointia tarjoaville palveluille, jotta sähköisiä tietoja ja sähköisiä asiakirjoja ja niihin liittyviä luottamuspalveluja voidaan säilyttää pitkällä aikavälillä. Jotta oikeusvarmuus, luottamus ja yhdenmukaistaminen voidaan varmistaa kaikissa jäsenvaltioissa, olisi vahvistettava hyväksytyjä sähköisiä arkistointipalveluja koskeva oikeudellinen kehys, joka perustuu tässä asetuksessa säädettyyn muita luottamuspalveluja koskevaan kehykseen. Hyväksytyjä sähköisiä arkistointipalveluja koskevan oikeudellisen kehyksen olisi tarjottava luottamuspalvelun tarjoajille ja käyttäjille tehokas välineistö, jossa huomioidaan sähköisen arkistointipalvelun toiminnalliset vaatimukset sekä selkeät oikeusvaikutukset, kun käytetään hyväksytyä sähköistä arkistointipalvelua. Kyseisiä säännöksiä olisi sovellettava sähköisiin tietoihin ja sähköisessä muodossa luotuihin sähköisiin asiakirjoihin sekä paperiasiakirjoihin, jotka on skannattu ja digitoitu. Kyseisten säännösten olisi tarvittaessa sallittava säilytettyjen sähköisten tietojen ja sähköisten asiakirjojen siirtäminen eri tallennusvälineille tai -muodoille, jotta niiden kestävyyttä ja luettavuutta voidaan jatkaa teknologista voimassaoloaikaan pidemmälle, samalla kun tietojen häviämistä ja muuttumista ehkäistään mahdollisuuksien mukaan. Jos sähköiseen arkistointipalveluun toimitetut sähköiset tiedot ja sähköiset asiakirjat sisältävät yhden tai useamman hyväksytyyn sähköisen allekirjoituksen tai hyväksytyyn sähköisen leiman, palvelun olisi käytettävä menettelyjä ja teknologioita, joilla voidaan pidentää niiden luotettavuutta tällaisten tietojen säilyttämisaikaa verran, mahdollisesti käyttämällä muita tällä asetuksella vahvistettuja hyväksytyjä luottamuspalveluja. Jotta voidaan luoda säilyttämistä koskevaa näyttöä sähköisten allekirjoitusten, sähköisten leimojen tai sähköisten aikaleimojen käytön osalta olisi käytettävä hyväksytyjä luottamuspalveluja. Siltä osin kuin sähköisiä arkistointipalveluja ei yhdenmukaisteta tällä asetuksella, jäsenvaltioilla olisi oltava mahdollisuus pitää voimassa tai ottaa käyttöön kyseisiä palveluja koskevia unionin oikeuden mukaisia kansallisia säännöksiä, kuten erityissäännöksiä, jotka koskevat organisaatioon integroituja palveluja ja joita käytetään vain kyseisen organisaation sisäisissä arkistoissa. Tässä asetuksessa ei saisi tehdä eroa sähköisten tietojen ja sähköisessä muodossa luotujen sähköisten asiakirjojen ja digitoitujen fyysisten asiakirjojen välillä.

- (67) Kansallisten arkistojen ja muistiorganisaatioiden eli organisaatioiden, jotka on omistettu asiakirjaperinnön säilyttämiselle yleisen edun vuoksi, toimintaa säädellään yleensä kansallisella lainsäädännöllä ja ne eivät välttämättä tarjoa tässä asetuksessa tarkoitettuja luottamuspalveluja. Siltä osin kuin tällaiset laitokset eivät tarjoa tällaisia luottamuspalveluja, tämä asetus ei vaikuta niiden toimintaan.
- (68) Sähköiset tilikirjat ovat sarja sähköisiä tietueita, joilla olisi varmistettava tietojen eheys ja kronologisen järjestyksen oikeellisuus. Sähköisten tilikirjojen olisi muodostettava kronologinen sarja tietueita. Yhdessä muiden teknologioiden kanssa niiden olisi edistettävä ratkaisuja tehokkaampien ja muutosvoimaisempien julkisten palvelujen luomiseksi, kuten sähköinen äänestämisen, tulliviranomaisten rajatylittävä yhteistyö, akateemisten laitosten rajatylittävä yhteistyö ja kiinteistöjen omistusoikeuden kirjaaminen hajautettuihin maarekistereihin. Hyväksytyjen sähköisten tilikirjojen olisi luotava oikeudellinen oletettava tilikirjan tietueiden yksilöllisestä ja oikeellisesta peräkkäisestä kronologisesta järjestyksestä ja eheydestä. Sähköisten tilikirjojen erityisattribuuteista, kuten tietueiden peräkkäisestä kronologisesta järjestyksestä, johtuen sähköiset tilikirjat olisi erotettava muista luottamuspalveluista, kuten sähköisistä aikaleimoista ja sähköisistä rekisteröidyistä jakelupalveluista. Oikeusvarmuuden varmistamiseksi ja innovoinnin edistämiseksi olisi luotava unionin laajuinen oikeudellinen kehys, jossa säädetään luottamuspalvelujen rajatylittävästä tunnustamisesta tietojen tallentamiseksi sähköisiin tilikirjoihin. Tämän olisi riittävällä tavalla estettävä saman digitaalisen omaisuuden kopiointi ja myynti eri osapuolille useammin kuin kerran. Sähköisen tilikirjan laatimis- ja päivittämisprosessi riippuu käytetyn tilikirjan tyyppistä eli siitä, onko se keskitetty vai jaettu. Tällä asetuksella olisi varmistettava teknologianeutraalius eli se, ettei suosita eikä syrjitä mitään teknologiaa, jota käytetään uuden sähköisten tilikirjojen luottamuspalvelun toteuttamiseen. Lisäksi komission olisi asianmukaisia menetelmiä käyttäen otettava huomioon ilmaston kohdistuvia haitallisia vaikutuksia tai muita ympäristöön liittyviä haitallisia vaikutuksia koskevat kestävyysindikaattorit, kun se laatii täytäntöönpanosäädöksiä, joissa täsmennetään hyväksytyjä sähköisiä tilikirjoja koskevat vaatimukset.

- (69) Sähköisten tilikirjojen luottamuspalvelun tarjoajien tehtävä olisi varmistaa tietojen peräkkäinen kirjaaminen tilikirjaan. Tämä asetus ei vaikuta sähköisten tilikirjojen käyttäjien unionin oikeuden tai kansallisen lainsäädännön mukaisiin oikeudellisiin velvoitteisiin. Esimerkiksi käyttötapauksissa, joihin liittyy henkilötietojen käsittelyä, olisi noudatettava asetusta (EU) 2016/679, ja rahoituspalveluihin liittyvien käyttötapauksien olisi oltava asiaankuuluvan unionin rahoituspalvelulainsäädännön mukaisia.
- (70) Jotta voidaan välttää erilaisista standardeista ja teknisistä rajoituksista johtuva sisämarkkinoiden hajanaisuus ja esteet ja varmistaa koordinoitu prosessi ja jotta ei vaikuteta eurooppalaisen digitaalisen identiteetin kehityksen täytäntöönpanoon, tarvitaan komission, jäsenvaltioiden, kansalaisyhteiskunnan, tiedeyhteisön ja yksityisen sektorin välistä tiivistä ja jäsenneiltyä yhteistyötä. Tämän tavoitteen saavuttamiseksi jäsenvaltioiden ja komission olisi tehtävä yhteistyötä komission suosituksessa (EU) 2021/946¹⁶ vahvistetuissa puitteissa, jotta voidaan määrittää välineistö eurooppalaista digitaalisen identiteetin kehystä varten. Jäsenvaltioiden olisi tässä yhteydessä sovittava kattavasta teknisestä arkkitehtuurista ja viitekehuksesta, yhteisistä standardeista ja teknisistä viiteasiakirjoista, mukaan lukien tunnustetut olemassa olevat standardit, sekä parhaita käytäntöjä koskevista suuntaviivoista ja kuvauksista, jotka kattavat vähintään kaikki eurooppalaisten digitaalisen identiteetin lompakoiden toiminnot ja yhteentoimivuuden, sähköiset allekirjoitukset mukaan luettuina, sekä tässä asetuksessa tarkoitettuja sähköisiä attribuuttitodistuksia tarjoavan hyväksytyt luottamuspalvelun. Tässä yhteydessä jäsenvaltioiden olisi myös päästävä sopimukseen eurooppalaisten digitaalisen identiteetin lompakoiden liiketoimintamallin ja maksurakenteen yhteisistä osatekijöistä lompakoiden käyttöönoton helpottamiseksi rajatylittävissä yhteyksissä erityisesti pk-yrityksissä. Välineistön sisältöä olisi kehitettävä rinnakkain eurooppalaista digitaalisen identiteetin kehystä koskevan keskustelun ja hyväksymisprosessin kanssa ja siinä olisi otettava huomioon niiden tulokset.

¹⁶ Komission suositus (EU) 2021/946, annettu 3 päivänä kesäkuuta 2021, unionin yhteisestä välineistöstä eurooppalaista digitaalisen identiteetin kehystä koskevaa koordinoitua lähestymistapaa varten (EUVL L 210, 14.6.2021, s. 51).

- (71) Tässä asetuksessa säädetään hyväksytyjen luottamuspalvelujen laadun, luotettavuuden ja turvallisuuden yhdenmukaisesta tasosta riippumatta siitä, missä toimintaa harjoitetaan. Hyväksytyyn luottamuspalvelun tarjoajan olisi voitava ulkoistaa hyväksytyyn luottamuspalvelun tarjoamiseen liittyvät toimensa kolmanteen maahan, jos kyseinen kolmas maa antaa riittävät takeet ja varmistaa, että valvontatoimet ja tarkastukset voidaan panna täytäntöön ikään kuin ne suoritettaisiin unionissa. Jos tämän asetuksen noudattamista ei voida täysin varmistaa, valvontaelinten olisi voitava hyväksyä oikeasuhtaisia ja perusteltuja toimenpiteitä, mukaan lukien luottamuspalvelulle annetun hyväksytyyn aseman peruuttaminen.
- (72) Kehittyneen ja hyväksytyyn varmenteeseen perustuvan sähköisen allekirjoituksen pätevyyttä koskevan oikeusvarmuuden varmistamiseksi on tärkeää, että kyseisen hyväksytyihin varmenteisiin perustuvan kehittyneen sähköisen allekirjoituksen validoinnin suorittavan luottavan osapuolen tekemä arviointi määritellään.
- (73) Luottamuspalvelujen tarjoajien olisi käytettävä salausmenetelmiä nykyisten parhaiden käytäntöjen mukaisesti ja kyseisten algoritmien luotettavaa täytäntöönpanoa voidakseen varmistaa luottamuspalvelujensa turvallisuuden ja luotettavuuden.

(74) Tässä asetuksessa säädetään hyväksytyjen luottamuspalvelun tarjoajien velvollisuudesta todentaa sellaisen luonnollisen henkilön tai oikeushenkilön henkilöllisyys, jolle hyväksytyt varmenne tai hyväksyty sähköinen attribuuttitodistus on myönnetty, käyttäen unionissa yhdenmukaistettuja eri menetelmiä. Sen varmistamiseksi, että hyväksytyt varmenteet ja hyväksytyt sähköiset attribuuttitodistukset myönnetään henkilölle, jolle ne kuuluvat, ja että niissä todistetaan kyseisen henkilön henkilöllisyyttä kuvaavat oikeat ja yksilölliset tiedot, hyväksytyjä varmenteita tai hyväksytyjä sähköisiä attribuuttitodistuksia myöntävien hyväksytyjen luottamuspalvelun tarjoajien olisi kyseisiä varmenteita ja todistuksia myöntäessään varmistettava, että kyseessä oleva henkilö tunnistetaan täydellä varmuudella. Henkilön henkilöllisyyden pakollisen todentamisen lisäksi ja sovellettavissa tapauksissa, kun on kyse hyväksytyjen varmenteiden ja hyväksytyjen sähköisten attribuuttitodistusten myöntämisestä, hyväksytyjen luottamuspalvelun tarjoajien olisi todennettava täydellä varmuudella sen henkilön varmennettujen attribuuttien oikeellisuus ja paikkansapitävyys, jolle hyväksyty varmenne tai hyväksyty sähköinen attribuuttitodistus on myönnetty. Näitä tulosvelvoitteita ja täydellistä varmuutta todistettujen tietojen todentamisessa olisi tuettava asianmukaisin keinoin, muun muassa käyttämällä yhtä tässä asetuksessa säädettyä menetelmää tai tarvittaessa menetelmien yhdistelmää. Näitä menetelmiä olisi voitava yhdistää, jotta voidaan luoda asianmukainen perusta sen henkilön henkilöllisyyden todentamiselle, jolle hyväksyty varmenne tai hyväksyty sähköinen attribuuttitodistus on myönnetty. Tällaiseen yhdistelmään olisi voitava sisältyä turvautuminen korotetun varmuustason vaatimukset täyttäviin sähköisen tunnistamisen menetelmiin yhdessä muiden henkilöllisyyden todentamiskeinojen kanssa. Tällainen sähköinen tunnistaminen mahdollistaisi tässä asetuksessa säädettyjen yhdenmukaistettujen vaatimusten täyttymisen korkean varmuustason osalta osana yhdenmukaistettuja etämenettelyjä, joilla varmistetaan tunnistamisen korkea luottamustaso. Näihin menetelmiin olisi sisällyttävä hyväksytyn sähköisen attribuuttitodistuksen myöntävän hyväksytyn luottamuspalvelun tarjoajan mahdollisuus todentaa attribuutit, jotka on todennettava sähköisesti käyttäjän pyynnöstä unionin oikeuden tai kansallisen lainsäädännön mukaisesti, myös käyttämällä virallisia lähteitä.

- (75) Jotta voidaan pitää tämä asetus globaalin kehityksen mukaisena ja noudattaa sisämarkkinoiden parhaita käytäntöjä, komission hyväksymiä delegoituja säädöksiä ja täytäntöönpanosäädöksiä olisi säännöllisesti tarkasteltava uudelleen ja tarvittaessa ajantasaistettava. Kyseisten päivitysten tarpeellisuuden arvioinnissa olisi otettava huomioon uudet teknologiat, käytännöt, standardit tai tekniset eritelvät.
- (76) Jäsenvaltiot eivät voi riittävällä tavalla saavuttaa tämän asetuksen tavoitteita, eli unionin laajuisen eurooppalaisen digitaalisen identiteetinkehityksen ja luottamuspalvelukehityksen kehittämistä, vaan ne voidaan sen laajuuden ja vaikutusten vuoksi saavuttaa paremmin unionin tasolla. Sen vuoksi unioni voi toteuttaa toimenpiteitä Euroopan unionista tehdyn sopimuksen 5 artiklassa vahvistetun toissijaisuusperiaatteen mukaisesti. Mainitussa artiklassa vahvistetun suhteellisuusperiaatteen mukaisesti tässä asetuksessa ei ylitetä sitä, mikä on tarpeen kyseisten tavoitteiden saavuttamiseksi.
- (77) Euroopan tietosuojavaltuutettua on kuultu asetuksen (EU) 2018/1725 42 artiklan 1 kohdan mukaisesti.
- (78) Asetus (EU) N:o 910/2014 olisi sen vuoksi muutettava vastaavasti,

OVAT HYVÄKSYNEET TÄMÄN ASETUKSEN:

1 artikla
Asetuksen (EU) N:o 910/2014 muuttaminen

Muutetaan asetusta (EU) N:o 910/2014 seuraavasti:

1) korvataan 1 artikla seuraavasti:

”1 artikla

Kohde

Tällä asetuksella pyritään varmistamaan sisämarkkinoiden moitteeton toiminta ja tietoturvan riittävän korkea taso kaikkialla unionissa käytettäville sähköisen tunnistamisen menetelmille ja luottamuspalveluille, jotta luonnolliset henkilöt ja oikeushenkilöt voivat käyttää oikeuttaan osallistua digitaaliyhteiskuntaan turvallisesti ja hyödyntää julkisia ja yksityisiä verkkopalveluja kaikkialla unionissa. Tätä varten tässä asetuksessa

- a) säädetään edellytyksistä, joiden mukaisesti jäsenvaltiot tunnustavat luonnollisten henkilöiden ja oikeushenkilöiden sähköisen tunnistamisen menetelmät, jotka kuuluvat toisen jäsenvaltion ilmoitetun sähköisen tunnistamisen järjestelmän piiriin, ja tarjoavat ja tunnustavat eurooppalaisia digitaalisen identiteetin lompakoita;
- b) säädetään luottamuspalveluja koskevista säännöistä erityisesti sähköisten transaktioiden osalta;
- c) vahvistetaan oikeudelliset puitteet sähköisille allekirjoituksille, sähköisille leimoille, sähköisille aikaleimoille, sähköisille asiakirjoille, sähköisille rekisteröidyille jakelupalveluille, verkkosivustojen todentamisen varmennepalveluille, sähköiselle arkistoinnille, sähköisille attribuuttitodistuksille, sähköisen allekirjoituksen luontivälineille, sähköisen leiman luontivälineille ja sähköisille tilikirjoille.”;

2) muutetaan 2 artikla seuraavasti:

a) korvataan 1 kohta seuraavasti:

”1. Tätä asetusta sovelletaan jäsenvaltion ilmoittamiin sähköisen tunnistamisen järjestelmiin, jäsenvaltion tarjoamiin eurooppalaisiin digitaalisen identiteetin lompakoihin ja unioniin sijoittautuneisiin luottamuspalvelujen tarjoajiin.”;

b) korvataan 3 kohta seuraavasti:

”3. Tämä asetus ei vaikuta unionin eikä kansalliseen oikeuteen, joka liittyy sopimusten tekemiseen ja pätevyyteen, muihin muotovaatimuksia koskeviin oikeudellisiin tai menettelyllisiin velvoitteisiin taikka alakohtaisiin muotovaatimuksiin.

4. Tämä asetus ei rajoita Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679* soveltamista.

* Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EUVL L 119, 4.5.2016, s. 1).”;

3) muutetaan 3 artikla seuraavasti:

a) korvataan 1–5 kohta seuraavasti:

- ”1) ’sähköisellä tunnistamisella’ prosessia, jossa käytetään tiettyä luonnollista henkilöä, oikeushenkilöä taikka toista luonnollista henkilöä tai oikeushenkilöä edustavaa luonnollista henkilöä vastaavia yksilöiviä tunnistetietoja sähköisessä muodossa;
- 2) ’sähköisen tunnistamisen menetelmällä’ aineellista ja/tai aineetonta kokonaisuutta, joka sisältää henkilön tunnistetietoja ja jota käytetään verkkopalveluun tai tapauksen mukaan verkon ulkopuoliseen palveluun liittyvään todentamiseen;
- 3) ’henkilön tunnistetiedoilla’ tietoja, jotka on annettu unionin oikeuden tai kansallisen lainsäädännön mukaisesti ja jotka mahdollistavat luonnollisen henkilön, oikeushenkilön taikka toista luonnollista henkilöä tai oikeushenkilöä edustavan luonnollisen henkilön henkilöllisyyden toteamisen;
- 4) ’sähköisen tunnistamisen järjestelmällä’ sähköiseen tunnistamiseen liittyvää järjestelmää, jonka puitteissa sähköisen tunnistamisen menetelmiä myönnetään luonnollisille henkilöille, oikeushenkilöille taikka muita luonnollisia henkilöitä tai oikeushenkilöitä edustaville luonnollisille henkilöille;
- 5) ’todentamisella’ sähköistä prosessia, joka mahdollistaa luonnollisen henkilön tai oikeushenkilön sähköisen tunnistamisen vahvistamisen tai sähköisessä muodossa olevien tietojen alkuperän ja eheyden vahvistamisen;”;

b) lisätään kohta seuraavasti:

”5 a) ’käyttäjällä’ luonnollista henkilöä tai oikeushenkilöä taikka toista luonnollista henkilöä tai oikeushenkilöä edustavaa luonnollista henkilöä, joka käyttää tämän asetuksen mukaisesti tarjottuja luottamuspalveluja tai sähköisen tunnistamisen menetelmiä;”;

c) korvataan 6 kohta seuraavasti:

”6) ’luottavalla osapuolella’ luonnollista henkilöä tai oikeushenkilöä, joka luottaa sähköiseen tunnistamiseen, eurooppalaisiin digitaalisen identiteetin lompakoihin tai muihin sähköisen tunnistamisen menetelmiin taikka luottamuspalveluun;”;

d) korvataan 16 kohta seuraavasti:

”16) ’luottamuspalvelulla’ sähköistä palvelua, jota yleensä tarjotaan vastiketta vastaan ja joka koostuu mistä tahansa seuraavista:

a) sähköisten allekirjoitusten varmenteiden, sähköisten leimojen varmenteiden, verkkosivustojen todentamisen varmenteiden tai muiden luottamuspalvelujen tarjoamista koskevien varmenteiden myöntäminen;

b) sähköisten allekirjoitusten varmenteiden, sähköisten leimojen varmenteiden, verkkosivustojen todentamisen varmenteiden tai muiden luottamuspalvelujen tarjoamista koskevien varmenteiden validointi;

- c) sähköisten allekirjoitusten tai sähköisten leimojen luominen;
- d) sähköisten allekirjoitusten tai sähköisten leimojen validointi;
- e) sähköisten allekirjoitusten, sähköisten leimojen, sähköisten allekirjoitusten varmenteiden tai sähköisten leimojen varmenteiden säilyttäminen;
- f) sähköisen allekirjoituksen etäluontivälineiden tai sähköisen leiman etäluontivälineiden hallinnointi;
- g) sähköisten attribuuttitodistusten myöntäminen;
- h) sähköisten attribuuttitodistusten validointi;
- i) sähköisten aikaleimojen luominen;
- j) sähköisten aikaleimojen validointi;
- k) sähköisten rekisteröityjen jakelupalvelujen tarjoaminen;
- l) sähköisten rekisteröityjen jakelupalvelujen kautta toimitettujen tietojen ja niihin liittyvien todisteiden validointi;
- m) sähköisten tietojen ja sähköisten asiakirjojen sähköinen arkistointi;
- n) sähköisten tietojen tallentaminen sähköiseen tilikirjaan;”;

e) korvataan 18 alakohta seuraavasti:

”18) ’vaatimustenmukaisuuden arviointilaitoksella’ asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa määriteltyä vaatimustenmukaisuuden arviointilaitosta, joka on akkreditoitu kyseisen asetuksen mukaisesti päteväksi arvioimaan hyväksytyjen luottamuspalvelun tarjoajien ja niiden tarjoamien hyväksytyjen luottamuspalvelujen vaatimustenmukaisuus tai päteväksi sertifioimaan eurooppalaiset digitaalisen identiteetin lompakot tai sähköisen tunnistamisen menetelmät;”;

f) korvataan 21 alakohta seuraavasti:

”21) ’tuotteella’ laitteistoja tai ohjelmistoja taikka laitteistojen tai ohjelmistojen merkityksellisiä osia, jotka on tarkoitettu käytettäväksi sähköisen tunnistamisen ja luottamuspalvelujen tarjoamiseen;”;

g) lisätään alakohdat seuraavasti:

”23 a) ’hyväksytyllä sähköisen allekirjoituksen etäluontivälineellä’ hyväksytyä sähköisen allekirjoituksen luontivälinettä, jota hyväksytty luottamuspalvelun tarjoaja hallinnoi allekirjoittajan puolesta 29 a artiklan mukaisesti;

23 b) ’hyväksytyllä sähköisen leiman etäluontivälineellä’ hyväksytyä sähköisen leiman luontivälinettä, jota hyväksytty luottamuspalvelun tarjoaja hallinnoi leiman luoja puolesta 39 a artiklan mukaisesti; ”;

h) korvataan 38 alakohta seuraavasti:

”38) ’verkkosivustojen todentamisen varmenteella’ sähköistä todistusta, jonka avulla verkkosivusto voidaan todentaa ja joka liittyy verkkosivuston siihen luonnolliseen henkilöön tai oikeushenkilöön, jolle varmenne on myönnetty;”;

i) korvataan 41 alakohta seuraavasti:

”41) ’validoinnilla’ prosessia sen tarkistamiseksi ja vahvistamiseksi, että sähköisessä muodossa olevat tiedot ovat päteviä tämän asetuksen mukaisesti;”;

j) lisätään alakohdat seuraavasti:

”42) ’eurooppalaisella digitaalisen identiteetin lompakolla’ sähköisen tunnistamisen menetelmää, jonka avulla käyttäjä voi turvallisesti tallentaa, hallinnoida ja validoida henkilön tunnistetietoja ja sähköisiä attribuuttitodistuksia niiden tarjoamiseksi luottaville osapuolille ja muille eurooppalaisten digitaalisen identiteetin lompakkojen käyttäjille sekä allekirjoittaa hyväksytyjen sähköisten allekirjoitusten tai leimata hyväksytyjen sähköisten leimojen avulla;

43) ’attribuutilla’ luonnollisen henkilön, oikeushenkilön tai esineen ominaispiirrettä, laatua, oikeutta tai lupaa;

44) ’sähköisellä attribuuttitodistuksella’ sähköisessä muodossa olevaa todistusta, joka mahdollistaa attribuuttien todentamisen;

- 45) 'hyväksytyllä sähköisellä attribuuttitodistuksella' sähköistä attribuuttitodistusta, jonka on myöntänyt hyväksytty luottamuspalvelujen tarjoaja ja joka täyttää liitteessä V säädetyt vaatimukset;
- 46) 'virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämällä tai sen puolesta myönnettyllä sähköisellä attribuuttitodistuksella' sähköistä attribuuttitodistusta, jonka on myöntänyt virallisesta lähteestä vastaava julkisen sektorin elin tai julkisen sektorin elin, jonka jäsenvaltio on nimennyt myöntämään tällaisia attribuuttitodistuksia niiden julkisen sektorin elinten puolesta, jotka vastaavat virallisista lähteistä 45 f artiklan ja liitteen VII mukaisesti;
- 47) 'virallisella lähteellä' julkisen sektorin elimen tai yksityisen tahon vastuulla ylläpidettyä rekisteriä tai järjestelmää, joka sisältää ja tarjoaa luonnollisten henkilöiden tai oikeushenkilöiden tai asioiden attribuutteja ja jota pidetään näiden tietojen ensisijaisena lähteenä tai joka tunnustetaan viralliseksi unionin oikeuden tai kansallisen lainsäädännön mukaisesti, mukaan lukien hallintokäytännöt;
- 48) 'sähköisellä arkistoinnilla' palvelua, jolla varmistetaan sähköisten tietojen ja sähköisten asiakirjojen vastaanotto, tallentaminen, hakeminen ja poistaminen, jotta voidaan varmistaa niiden pysyvyys ja luettavuus sekä säilyttää niiden eheys ja luottamuksellisuus ja todistus alkuperästä koko säilytysajan;
- 49) 'hyväksytyllä sähköisellä arkistointipalvelulla' sähköistä arkistointipalvelua, jonka hyväksytty luottamuspalvelujen tarjoaja tarjoaa ja joka täyttää 45 j artiklassa säädetyt vaatimukset;

- 50) 'EU:n digitaalisen identiteetin lompakon luotettavuusmerkillä' tarkastettavissa olevaa, yksinkertaista, tunnistettavaa ja selkeästi viestittyä osoitusta siitä, että eurooppalainen digitaalisen identiteetin lompakko on tarjottu tämän asetuksen mukaisesti;
- 51) 'käyttäjän vahvalla todentamisella' todentamista, jossa käytetään todentamistietojen luottamuksellisuuden suojaamiseksi menettelyä, joka perustuu vähintään kahteen toisistaan riippumattomaan todentamistekijään, jotka kuuluvat eri ryhmiin, jotka ovat tieto eli jotain, minkä vain käyttäjä tietää, hallussapito eli jotain, mitä vain käyttäjällä on hallussaan, tai erityinen ominaisuus eli jotain, mitä käyttäjä on siten, että yhden rikkominen ei aseta kyseenalaiseksi muiden luotettavuutta;
- 52) 'sähköisellä tilikirjalla' sarjaa sähköisiä tietueita, joilla varmistetaan kyseisten tietueiden eheys ja kyseisten tietueiden kronologisen järjestyksen oikeellisuus;
- 53) 'hyväksytyllä sähköisellä tilikirjalla' sähköistä tilikirjaa, jonka hyväksytty luottamuspalvelujen tarjoaja tarjoaa ja joka täyttää 45 l artiklassa säädetyt vaatimukset;
- 54) 'henkilötiedoilla' asetuksen (EU) 2016/679 4 artiklan 1 alakohdassa määritellyjä tietoja;

- 55) 'henkilöllisyyden linkittämisellä' prosessia, jossa henkilön tunnistetiedot tai sähköiset tunnistamismenetelmät yhdistetään tai liitetään samalle henkilölle kuuluvaan olemassa olevaan tiliin;
- 56) 'tietueella' sähköisiä tietoja, jotka on tallennettu tietojen käsittelyä tukevien metatietojen kera;
- 57) 'verkon ulkopuolella' eurooppalaisten digitaalisen identiteetin lompakoiden osalta käyttäjän ja kolmannen osapuolen välistä vuorovaikutusta fyysisessä paikassa lähiteknologiaa käyttäen, jolloin eurooppalaiselta digitaalisen identiteetin lompakolta ei vaadita pääsyä etäjärjestelmiin sähköisten viestintäverkkojen kautta vuorovaikutusta varten.”;

4) korvataan 5 artikla seuraavasti:

”5 artikla

Pseudonyymien käyttö sähköisissä transaktioissa

Käyttäjän valitsemien pseudonyymien käyttöä ei kielletä, sanotun kuitenkin rajoittamatta niiden unionin oikeuden tai kansallisen lainsäädännön erityisten sääntöjen soveltamista, joiden mukaan käyttäjien on tunnistauduttava, tai pseudonyymeille kansallisessa laissa annettavia oikeusvaikutuksia.”;

5) lisätään II lukuun jakso seuraavasti:

”1 JAKSO

EUROOPPALAINEN DIGITAALISEN IDENTITEETIN LOMPAKKO

5 a artikla

Eurooppalaiset digitaalisen identiteetin lompakot

1. Sen varmistamiseksi, että kaikilla luonnollisilla ja oikeushenkilöillä unionissa on turvallinen, luotettava ja saumaton rajatylittävä pääsy julkisiin ja yksityisiin palveluihin ja täysi määräysvalta tietoihinsa, kunkin jäsenvaltion on tarjottava vähintään yksi eurooppalainen digitaalisen identiteetin lompakko 24 kuukauden kuluessa tämän artiklan 23 kohdassa ja 5 c artiklan 6 kohdassa tarkoitettujen täytäntöönpanosäädösten voimaantulopäivästä.
2. Eurooppalaiset digitaalisen identiteetin lompakot tarjotaan jollakin seuraavista tavoista:
 - a) suoraan jäsenvaltion toimesta;
 - b) jäsenvaltion toimeksiannosta;
 - c) jäsenvaltiosta riippumatta mutta niin, että kyseinen jäsenvaltio tunnustaa sen.
3. Eurooppalaisten digitaalisen identiteetin lompakoiden sovellusten ohjelmistokomponenttien lähdekoodin on oltava avoimen lähdekoodin mukaisesti lisensoitu. Jäsenvaltiot voivat säätää, että asianmukaisesti perustelluista syistä muiden kuin käyttäjien laitteisiin asennettujen tiettyjen komponenttien lähdekoodia ei saa luovuttaa.

4. Eurooppalaisten digitaalisen identiteetin lompakkojen avulla käyttäjän on voitava käyttäjäystävällisellä, läpinäkyvällä ja käyttäjän jäljitettävissä olevalla tavalla
- a) turvallisesti pyytää, saada, valita, yhdistää, tallentaa, poistaa, jakaa ja esittää käyttäjän yksinomaisessa hallinnassa henkilön tunnistetietoja ja tapauksen mukaan yhdessä sähköisten attribuuttitodistusten kanssa todentautua luottaville osapuolille verkossa ja tapauksen mukaan verkon ulkopuolella julkisten ja yksityisten palvelujen käyttämiseksi, varmistaen samalla, että tietojen valikoiva luovuttaminen on mahdollista;
 - b) muodostaa pseudonyymejä ja tallentaa ne salattuina ja paikallisesti eurooppalaiseen digitaalisen identiteetin lompakkoon;
 - c) turvallisesti todentaa toisen henkilön eurooppalainen digitaalisen identiteetin lompakko ja vastaanottaa ja jakaa henkilön tunnistetietoja ja sähköisiä attribuuttitodistuksia turvallisesti kahden eurooppalaisen digitaalisen identiteetin lompakon välillä;
 - d) päästä kaikkien eurooppalaisen digitaalisen identiteetin lompakon kautta suoritettujen transaktioiden lokiin yhteisen ohjauspaneelin kautta, jonka avulla käyttäjä voi
 - i) tarkastella ajantasaista luetteloa luottavista osapuolista, joihin käyttäjä on luonut yhteyden, ja soveltuvissa tapauksissa kaikkea jaettua tietoa;
 - ii) helposti pyytää, että luottava osapuoli poistaa henkilötietoja asetuksen (EU) 2016/679 17 artiklan mukaisesti;
 - iii) raportoida helposti luottavasta osapuolesta kansalliselle toimivaltaiselle tietosuojaviranomaiselle, jos vastaanotettu tietopyyntö on väitetysti lainvastainen tai epäilyttävä;

- e) allekirjoittaa hyväksytyillä sähköisillä allekirjoituksilla tai leimata käyttäen hyväksytyjä sähköisiä leimoja;
 - f) ladata, siinä määrin kuin se on teknisesti mahdollista, käyttäjän tiedot, sähköiset attribuuttitodistukset ja konfiguraatiot;
 - g) käyttää käyttäjän oikeutta tietojen siirtoon.
5. Eurooppalaisten digitaalisen identiteetin lompakoiden on erityisesti
- a) tuettava yhteisiä protokollia ja rajapintoja:
 - i) henkilön tunnistetietojen, hyväksytyjen ja ei-hyväksytyjen sähköisten attribuuttitodistusten tai hyväksytyjen ja ei-hyväksytyjen varmenteiden myöntämiseksi eurooppalaiseen digitaaliseen identiteetin lompakkoon;
 - ii) luottaville osapuolille, jotta ne voivat pyytää ja validoida henkilön tunnistetietoja ja sähköisiä attribuuttitodistuksia;
 - iii) henkilöiden tunnistetietojen, sähköisten attribuuttitodistusten tai näihin liittyvän valikoiden luovutettavan tiedon jakamiseksi ja esittämiseksi luottaville osapuolille verkossa ja soveltuviissa tapauksissa verkon ulkopuolella;
 - iv) jotta käyttäjä voi sallia vuorovaikutuksen eurooppalaisen digitaalisen identiteetin lompakon kanssa ja näyttää EU:n digitaalisen identiteetin lompakon luotettavuusmerkin;

- v) käyttäjien turvallisen käyttösuhteen aloittamiseksi käyttämällä 5 a artiklan 24 kohdan mukaista sähköisen tunnistamisen menetelmää;
 - vi) vuorovaikutukseen kahden henkilön eurooppalaisten digitaalisen identiteetin lompakoiden välillä tarkoituksena vastaanottaa, validoida ja jakaa henkilön tunnistetietoja ja sähköisiä attribuuttitodistuksia turvallisesti;
 - vii) luottavien osapuolten todentamiseksi ja tunnistamiseksi ottamalla käyttöön todentamismekanismit 5 b artiklan mukaisesti;
 - viii) luottaville osapuolille eurooppalaisten digitaalisen identiteetin lompakkojen aitouden ja voimassaolon tarkistamiseksi;
 - ix) pyynnön esittämiseksi luottavalle osapuolelle henkilötietojen poistamiseksi asetuksen (EU) 2016/679 17 artiklan mukaisesti;
 - x) luottavasta osapuolesta raportoimiseksi toimivaltaiselle kansalliselle tietosuojaviranomaiselle, jos vastaanotettu tietopyyntö on väitetysti lainvastainen tai epäilyttävä;
 - xi) hyväksytyjen sähköisten allekirjoitusten tai sähköisten leimojen luomiseksi hyväksytyjen sähköisten allekirjoitusten tai sähköisten leimojen luontivälineiden avulla;
- b) oltava antamatta sähköisiä attribuuttitodistuksia myöntäville luottamuspalvelun tarjoajille mitään tietoja kyseisten sähköisten todistusten käytöstä;

- c) varmistettava, että luottavat osapuolet voidaan todentaa ja tunnistaa ottamalla käyttöön todentamismekanismeja 5 b artiklan mukaisesti;
- d) täytettävä 8 artiklassa vahvistetut vaatimukset korkean varmuustason osalta, erityisesti siltä osin kuin sitä sovelletaan henkilöllisyyden todistamista ja varmentamista sekä sähköisen tunnistamisen menetelmien hallintaa ja todentamista koskeviin vaatimuksiin;
- e) kun on kyse sähköisistä attribuuttitodistuksista, joissa on sisäänrakennettuja tietojen luovuttamiskäytäntöjä, otettava käyttöön asianmukainen mekanismi, jolla ilmoitetaan käyttäjälle, että kyseisiä sähköisiä attribuuttitodistuksia pyytävällä luottavalla osapuolella tai eurooppalaisen digitaalisen identiteetin lompakon käyttäjällä on lupa tällaisten todistusten käyttöön;
- f) varmistettava, että henkilön tunnistetiedot, jotka ovat saatavilla sähköisen tunnistamisen järjestelmästä, jonka puitteissa eurooppalainen digitaalisen identiteetin lompakko tarjotaan, edustavat yksilöivästi luonnollista henkilöä, oikeushenkilöä taikka luonnollista henkilöä tai oikeushenkilöä edustavaa luonnollista henkilöä ja liittyvät kyseiseen eurooppalaiseen digitaalisen identiteetin lompakkoon;
- g) tarjottava oletusarvoisesti ja maksutta kaikille luonnollisille henkilöille valmiudet allekirjoittamiseen hyväksytyjen sähköisten allekirjoitusten avulla.

Sen estämättä, mitä ensimmäisen alakohdan g alakohdassa säädetään, jäsenvaltiot voivat säätää oikeasuhteisista toimenpiteistä sen varmistamiseksi, että luonnollisten henkilöiden maksutta tapahtuva hyväksytyjen sähköisten allekirjoitusten käyttö rajoitetaan muihin kuin ammatillisiin tarkoituksiin.

6. Jäsenvaltioiden on ilmoitettava käyttäjille ilman viivytystä mahdollisista tietoturvaloukkauksista, jotka ovat voineet kokonaan tai osittain vaarantaa heidän eurooppalaisen digitaalisen identiteetin lompakkonsa tai sen sisällön, erityisesti jos heidän eurooppalaisen digitaalisen identiteetin lompakkonsa voimassaolo on keskeytetty tai peruutettu 5 e artiklan mukaisesti.
7. Jäsenvaltiot voivat kansallisen lainsäädännön mukaisesti tarjota eurooppalaisten digitaalisen identiteetin lompakoiden lisätoimintoja, mukaan lukien yhteentoimivuus olemassa olevien kansallisten sähköisen tunnistamisen menetelmien kanssa, sanotun kuitenkin rajoittamatta 5 f artiklan soveltamista. Näiden lisätoimintojen on oltava tämän artiklan mukaisia.
8. Jäsenvaltioiden on tarjottava maksutta validointimekanismeja, jotta
 - a) varmistetaan, että eurooppalaisten digitaalisen identiteetin lompakkojen aitous ja voimassaolo voidaan tarkistaa;
 - b) annetaan käyttäjille mahdollisuus tarkistaa 5 b artiklan mukaisesti rekisteröityjen luottavien osapuolten henkilöllisyyden aitous ja kelpoisuus.
9. Jäsenvaltioiden on varmistettava, että eurooppalaisen digitaalisen identiteetin lompakon voimassaolo voidaan peruuttaa seuraavissa tilanteissa:
 - a) käyttäjän nimenomaisesta pyynnöstä;
 - b) eurooppalaisen digitaalisen identiteetin lompakon turvallisuuden vaarannuttua;
 - c) käyttäjän kuoltua tai oikeushenkilön toiminnan päätyttyä.

10. Eurooppalaisten digitaalisen identiteetin lompakkojen tarjoajien on varmistettava, että käyttäjät voivat helposti pyytää teknistä tukea ja raportoida teknisistä ongelmista tai muista poikkeamista, jotka vaikuttavat kielteisesti eurooppalaisen digitaalisen identiteetin lompakon käyttöön.
11. Eurooppalaiset digitaalisen identiteetin lompakot on tarjottava osana sähköisen tunnistamisen järjestelmää, jonka varmuustaso on korkea.
12. Eurooppalaisissa digitaalisen identiteetin lompakoissa on varmistettava sisäänrakennettu turvallisuus.
13. Eurooppalaisten digitaalisen identiteetin lompakoiden myöntämisen, käytön ja peruuttamisen on oltava maksutonta kaikille luonnollisille henkilöille.
14. Käyttäjillä on oltava täysi määräysvalta eurooppalaisen digitaalisen identiteetin lompakkonsa käyttöön ja sen sisältämiin tietoihin. Eurooppalaisen digitaalisen identiteetin lompakon tarjoaja ei saa kerätä eurooppalaisen digitaalisen identiteetin lompakon käytöstä tietoja, jotka eivät ole välttämättömiä eurooppalaisen digitaalisen identiteetin lompakon palvelujen tarjoamiseksi, eikä yhdistää henkilön tunnistetietoja eikä muita henkilötietoja, jotka on tallennettu tai jotka liittyvät eurooppalaisen digitaalisen identiteetin lompakon käyttöön, muihin kyseisen tarjoajan tai kolmansien osapuolten tarjoamista palveluista saatuihin henkilötietoihin, jotka eivät ole välttämättömiä eurooppalaisen digitaalisen identiteetin lompakon palvelujen tarjoamiseksi, paitsi jos käyttäjä on nimenomaisesti toisin pyytänyt. Eurooppalaisen digitaalisen identiteetin lompakon tarjoamiseen liittyvät henkilötiedot on pidettävä loogisesti erillään kaikista muista tiedoista, joita eurooppalaisen digitaalisen identiteetin lompakon tarjoajan hallussa on. Jos eurooppalaisen digitaalisen identiteetin lompakon tarjoavat yksityiset osapuolet tämän artiklan 2 kohdan b ja c alakohdan mukaisesti, sovelletaan 45 h artiklan 3 kohdan säännöksiä soveltuvien osin.

15. Eurooppalaisen digitaalisen identiteetin lompakon käytön on oltava vapaaehtoista. Julkisten ja yksityisten palvelujen saatavuutta, työmarkkinoille pääsyä ja elinkeinovapautta ei saa millään tavoin rajoittaa tai haitata sellaisten luonnollisten henkilöiden ja oikeushenkilöiden osalta, jotka eivät käytä eurooppalaista digitaalisen identiteetin lompakkoa. Julkisia ja yksityisiä palveluja on edelleen voitava käyttää muilla olemassa olevilla tunnistus- ja todentamismenetelmillä.
16. Eurooppalaisen digitaalisen identiteetin lompakon tekniset puitteet
- a) eivät saa johtaa siihen, että sähköisten attribuuttitodistusten tarjoajat tai jokin muu osapuoli pystyy attribuuttitodistuksen myöntämisen jälkeen saamaan tietoja, joiden avulla voidaan seurata, yhdistellä tai korreloida transaktioita tai käyttäjän käyttäytymistä, taikka muulla tavoin saamaan tietoja näistä, ellei käyttäjä ole antanut siihen nimenomaista lupaa;
 - b) mahdollistavat yksityisyyttä suojaavat tekniikat sen varmistamiseksi, ettei tietoja yhdistellä, jos attribuuttitodistus ei edellytä käyttäjän tunnistamista.
17. Kaikki henkilötietojen käsittely, jota suorittavat jäsenvaltiot tai näiden puolesta eurooppalaisten digitaalisen identiteetin lompakoiden tarjoamisesta sähköisen tunnistamisen menetelmänä vastaavat elimet tai osapuolet, on suoritettava asianmukaisten ja tehokkaiden tietosuojatoimenpiteiden mukaisesti. Tällaisen käsittelyn osalta on osoitettava, että asetusta (EU) 2016/679 noudatetaan. Jäsenvaltiot voivat ottaa käyttöön kansallisia säännöksiä, joissa täsmennetään tällaisten toimenpiteiden soveltamista.

18. Jäsenvaltioiden on ilman aiheetonta viivytystä ilmoitettava komissiolle seuraavat tiedot:

- a) elin, joka vastaa eurooppalaisia digitaalisen identiteetin lompakoita käyttävien rekisteröityjen luottavien osapuolten luettelon laatimisesta ja ylläpitämisestä 5 b artiklan 5 kohdan mukaisesti, sekä kyseisen luettelon sijainti;
- b) elimet, jotka vastaavat eurooppalaisten digitaalisen identiteetin lompakoiden tarjoamisesta 5 a artiklan 1 kohdan mukaisesti;
- c) elimet, jotka ovat vastuussa sen varmistamisesta, että henkilön tunnistetiedot liitetään eurooppalaiseen digitaalisen identiteetin lompakkoon 5 a artiklan 5 kohdan f alakohdan mukaisesti;
- d) mekanismi, joka mahdollistaa 5 a artiklan 5 kohdan f alakohdassa tarkoitettujen henkilöiden tunnistetietojen ja luottavien osapuolten henkilöllisyyden validoinnin;
- e) mekanismi, jolla validoidaan eurooppalaisten digitaalisen identiteetin lompakkojen aitous ja voimassaolo.

Komissio asettaa ensimmäisen alakohdan mukaisesti ilmoitetut tiedot suojatusti julkisesti saataville sähköisesti allekirjoitetussa tai leimatussa muodossa, joka soveltuu automaattiseen käsittelyyn.

19. Sanotun kuitenkin rajoittamatta tämän artiklan 22 kohdan soveltamista, tämän asetuksen 11 artiklaa sovelletaan soveltuvin osin eurooppalaiseen digitaalisen identiteetin lompakkoon.

20. Tämän asetuksen 24 artiklan 2 kohdan b ja d–h alakohtaa sovelletaan soveltuvin osin eurooppalaisten digitaalisen identiteetin lompakoiden tarjoajiin.
21. Eurooppalaisten digitaalisen identiteetin lompakoiden on oltava esteettömästi vammaisten henkilöiden käytettävissä yhdenvertaisesti muiden käyttäjien kanssa Euroopan parlamentin ja neuvoston direktiivin (EU) 2019/882* mukaisesti.
22. Eurooppalaisten digitaalisen identiteetin lompakoiden tarjoamiseksi eurooppalaisiin digitaalisen identiteetin lompakoihin ja sähköisen tunnistamisen järjestelmiin, joiden puitteissa niitä tarjotaan, ei sovelleta 7, 9, 10, 12 ja 12 a artiklassa säädettyjä vaatimuksia.
23. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [kuusi kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa eritelmät ja menettelyt tämän artiklan 4, 5, 8 ja 18 kohdassa tarkoitettuja vaatimuksia varten antamalla eurooppalaisen digitaalisen identiteetin lompakon toteuttamista koskevia täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

24. Antamalla täytäntöönpanosäädöksiä komissio vahvistaa luettelon viitestandardeista ja tarvittaessa eritelvät ja menettelyt, jotta voidaan helpottaa eurooppalaisen digitaalisen identiteetin lompakon käyttäjien käyttösuhteen aloittamista käyttäen joko korkean varmuustason mukaista sähköisen tunnistamisen menetelmää tai korotetun varmuustason mukaista sähköisen tunnistamisen menetelmää yhdessä sellaisten täydentävien käyttösuhteen aloittamisen etämenettelyjen kanssa, jotka yhdessä täyttävät korkean varmuustason vaatimukset. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

5 b artikla

Eurooppalaisen digitaalisen identiteetin lompakon luottavat osapuolet

1. Jos luottava osapuoli aikoo luottaa eurooppalaisiin digitaalisen identiteetin lompakoihin julkisten tai yksityisten palvelujen tarjoamiseksi digitaalisen vuoro vaikutuksen keinoin, luottavan osapuolen on rekisteröidyttävä siinä jäsenvaltiossa, johon se on sijoittautunut.
2. Rekisteröintimenettelyn on oltava kustannustehokas ja oikeassa suhteessa riskiin. Luottavan osapuolen on toimitettava vähintään
 - a) tiedot, joita tarvitaan todentautumiseksi eurooppalaisiin digitaalisen identiteetin lompakoihin ja joita ovat vähintään
 - i) jäsenvaltio, johon luottava osapuoli on sijoittautunut; ja
 - ii) luottavan osapuolen nimi ja tapauksen mukaan rekisterinumero virallisessa rekisterissä olevassa muodossa sekä kyseisen virallisen rekisterin tunnistetiedot;

- b) luottavan osapuolen yhteystiedot;
 - c) eurooppalaisten digitaalisen identiteetin lompakoiden käyttötarkoitus, mukaan lukien ilmoitus tiedoista, joita luottava osapuoli pyytää käyttäjiltä.
3. Luottavat osapuolet eivät saa pyytää käyttäjiä toimittamaan muita tietoja kuin niitä, jotka ilmoitetaan 2 kohdan c alakohdan mukaisesti.
 4. Edellä olevat 1 ja 2 kohta eivät rajoita sellaisen unionin oikeuden tai kansallisen lainsäädännön soveltamista, joka on sovellettavissa tiettyjen palvelujen tarjoamiseen.
 5. Jäsenvaltiot asettavat 2 kohdassa tarkoitetut tiedot julkisesti saataville verkkoon sähköisesti allekirjoitetussa tai leimatussa muodossa, joka soveltuu automaattiseen käsittelyyn.
 6. Tämän artiklan mukaisesti rekisteröityjen luottavien osapuolten on ilmoitettava jäsenvaltioille viipymättä kaikista muutoksista rekisteröinnin yhteydessä 2 kohdan mukaisesti annettuihin tietoihin.
 7. Jäsenvaltioiden on tarjottava yhteinen mekanismi, joka mahdollistaa 5 a artiklan 5 kohdan c alakohdassa tarkoitetun luottavien osapuolten tunnistamisen ja todentamisen.
 8. Jos luottavat osapuolet aikovat luottaa eurooppalaisiin digitaalisen identiteetin lompakoihin, niiden on tunnistauduttava käyttäjälle.

9. Luottavat osapuolet vastaavat sellaisen menettelyn toteuttamisesta, jolla todennetaan ja validoidaan henkilön tunnistetiedot ja sähköiset attribuuttitodistukset, joita pyydetään eurooppalaisista digitaalisen identiteetin lompakoista. Luottavat osapuolet eivät saa kieltää pseudonyymien käyttöä, jos unionin oikeudessa tai kansallisessa lainsäädännössä ei edellytetä käyttäjän tunnistamista.
10. Luottavien osapuolten puolesta toimivia välittäjiä on pidettävä luottavina osapuolina, eivätkä ne saa tallentaa tietoja transaktion sisällöstä.
11. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [kuusi kuukautta tämän muutosasetuksen voimaantulopäivästä] tekniset eritelvät ja menettelyt tämän artiklan 2, 5 ja 6–9 kohdassa tarkoitettuja vaatimuksia varten antamalla 5 a artiklan 23 kohdassa tarkoitettuja täytäntöönpanosäädöksiä eurooppalaisten digitaalisen identiteetin lompakoiden toteuttamisesta. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

5 c artikla

Eurooppalaisten digitaalisen identiteetin lompakoiden sertifiointi

1. Jäsenvaltioiden nimeämien vaatimustenmukaisuuden arviointilaitosten on sertifioidava se, että eurooppalaiset digitaalisen identiteetin lompakot ja sähköisen tunnistamisen järjestelmä, jonka puitteissa niitä tarjotaan, ovat 5 a artiklan 4, 5 ja 8 kohdassa säädettyjen vaatimusten, 5 a artiklan 14 kohdassa säädetyn loogista erillään pitoa koskevan vaatimuksen ja tarvittaessa 5 a artiklan 24 kohdassa tarkoitettujen standardien ja teknisten eritelmien mukaisia.

2. Sen sertifiointi, ovatko eurooppalaiset digitaalisen identiteetin lompakot tai niiden osat tämän artiklan 1 kohdassa tarkoitettujen kyberturvallisuuden kannalta merkityksellisten vaatimusten mukaisia, on suoritettava niiden eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisesti, jotka on hyväksytty Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881** nojalla ja joita tarkoitetaan tämän artiklan 6 kohdassa tarkoitetuissa täytäntöönpanosäädöksissä.
3. Tämän artiklan 1 kohdassa tarkoitettujen sellaisten vaatimusten osalta, jotka eivät ole merkityksellisiä kyberturvallisuuden kannalta, ja tämän artiklan 1 kohdassa tarkoitettujen sellaisten vaatimusten osalta, jotka ovat merkityksellisiä kyberturvallisuuden kannalta, siltä osin kuin tämän artiklan 2 kohdassa tarkoitettujen kyberturvallisuuden sertifiointijärjestelmät eivät kata kyseisiä kyberturvallisuusvaatimuksia tai kattavat ne vain osittain, jäsenvaltioiden on luotava myös kyseisiä vaatimuksia varten kansallisia sertifiointijärjestelmiä, jotka noudattavat tämän artiklan 6 kohdassa tarkoitetuissa täytäntöönpanosäädöksissä vahvistettuja vaatimuksia. Jäsenvaltioiden on toimitettava luonnoksensa kansallisiksi sertifiointijärjestelmiksi 46 e artiklan 1 kohdan nojalla perustetulle eurooppalaiselle digitaalisen identiteetin yhteistyöryhmälle, jäljempänä 'yhteistyöryhmä'. Yhteistyöryhmä voi antaa lausuntoja ja suosituksia.
4. Edellä olevan 1 kohdan mukainen sertifiointi on voimassa enintään viisi vuotta edellyttäen, että haavoittuvuusarviointi tehdään joka toinen vuosi. Jos haavoittuvuus havaitaan eikä sitä korjata kohtuullisessa ajassa, sertifiointi peruutetaan.
5. Henkilötietojen käsittelytoimiin liittyvien tämän asetuksen 5 a artiklassa vahvistettujen vaatimusten noudattaminen voidaan sertifioida asetuksen (EU) 2016/679 mukaisesti.

6. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [kuusi kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa eritelvät ja menettelyt tämän artiklan 1, 2 ja 3 kohdassa tarkoitettua eurooppalaisten digitaalisen identiteetin lompakoiden sertifiointia varten antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.
7. Jäsenvaltioiden on ilmoitettava komissiolle 1 kohdassa tarkoitettujen vaatimustenmukaisuuden arviointilaitosten nimet ja osoitteet. Komissio asettaa nämä tiedot kaikkien jäsenvaltioiden saataville.
8. Siirretään komissiolle valta antaa 47 artiklan mukaisesti delegoituja säädöksiä tämän artiklan 1 kohdassa tarkoitetuille nimetyille vaatimustenmukaisuuden arviointilaitoksille asetettavista erityisvaatimuksista.

5 d artikla

Sertifioitujen eurooppalaisten digitaalisen identiteetin lompakoiden luettelon julkaiseminen

1. Jäsenvaltioiden on ilman aiheetonta viivytystä ilmoitettava komissiolle ja 46 e artiklan 1 kohdalla perustetulle yhteistyöryhmälle eurooppalaisista digitaalisen identiteetin lompakoista, jotka on tarjottu 5 a artiklan mukaisesti ja jotka ovat 5 c artiklan 1 kohdassa tarkoitettujen vaatimustenmukaisuuden arviointilaitosten sertifiointia. Niiden on ilman aiheetonta viivytystä ilmoitettava komissiolle ja 46 e artiklan 1 kohdalla perustetulle yhteistyöryhmälle, jos sertifiointi peruutetaan, ja esitettävä peruuttamisen syyt.

2. Sanotun kuitenkin rajoittamatta 5 a artiklan 18 kohdan soveltamista, tämän artiklan 1 kohdassa tarkoitettuihin jäsenvaltioiden toimittamiin tietoihin on sisällyttävä vähintään
 - a) sertifioidun eurooppalaisen digitaalisen identiteetin lompakon sertifikaatti ja sertifiointin arviointiraportti;
 - b) kuvaus sähköisen tunnistamisen järjestelmästä, jonka puitteissa eurooppalainen digitaalisen identiteetin lompakko tarjotaan;
 - c) sovellettava valvontajärjestelmä ja tiedot vastuujärjestelmästä sen osapuolen osalta, joka vastaa eurooppalaisen digitaalisen identiteetin lompakon tarjoamisesta;
 - d) sähköisen tunnistamisen järjestelmästä vastaava viranomainen tai vastaavat viranomaiset;
 - e) keskeyttämis- tai peruuttamisjärjestelyt, kun on kyse sähköisen tunnistamisen järjestelmästä tai todentamisesta taikka asianomaisista osista, joiden turvallisuus on vaarantunut.
3. Edellä olevan 1 kohdan mukaisesti saamiensa tietojen perusteella komissio laatii luettelon sertifioiduista eurooppalaisista digitaalisen identiteetin lompakoista, julkaisee sen *Euroopan unionin virallisessa lehdessä* ja ylläpitää sitä koneellisesti luettavassa muodossa.
4. Jäsenvaltio voi toimittaa komissiolle pyynnön poistaa eurooppalainen digitaalisen identiteetin lompakko ja sähköisen tunnistamisen järjestelmä, jonka puitteissa sitä tarjotaan, 3 kohdassa tarkoitetusta luettelosta.
5. Jos 1 kohdan mukaisesti toimitettuihin tietoihin tehdään muutoksia, jäsenvaltion on toimitettava komissiolle ajantasaiset tiedot.

6. Komissio pitää 3 kohdassa tarkoitetun luettelon ajan tasalla julkaisemalla vastaavat muutokset luetteloon *Euroopan unionin virallisessa lehdessä* kuukauden kuluessa 4 kohdan mukaisen pyynnön tai 5 kohdan mukaisten ajantasaisten tietojen vastaanottamisesta.
7. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [kuusi kuukautta tämän muutosasetuksen voimaantulopäivästä] muutoseikat ja menettelyt, joita sovelletaan tämän artiklan 1, 4 ja 5 kohdan soveltamiseksi, antamalla 5 a artiklan 23 kohdassa tarkoitettuja täytäntöönpanosäädöksiä eurooppalaisten digitaalisen identiteetin lompakoiden toteuttamisesta. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

5 e artikla

Eurooppalaisten digitaalisen identiteetin lompakoiden tietoturvaloukkaus

1. Jos 5 a artiklan mukaisesti tarjottuihin eurooppalaisiin digitaalisen identiteetin lompakoihin, 5 a artiklan 8 kohdassa tarkoitettuihin validointimekanismeihin tai sähköisen tunnistamisen järjestelmään, jonka puitteissa eurooppalaisia digitaalisen identiteetin lompakoita tarjotaan, kohdistuu tietoturvaloukkaus tai jos niiden turvallisuus on osittain vaarantunut tavalla, joka vaikuttaa niiden luotettavuuteen tai muiden eurooppalaisten digitaalisen identiteetin lompakoiden luotettavuuteen, jäsenvaltion, joka on tarjonnut kyseiset eurooppalaiset digitaalisen identiteetin lompakot, on ilman aiheetonta viivytystä keskeytettävä kyseisten eurooppalaisten digitaalisen identiteetin lompakoiden tarjoaminen ja käyttö.

Jos se on perusteltua ensimmäisessä alakohdassa tarkoitetun tietoturvaloukkauksen tai vaarantumisen vakavuuden vuoksi, jäsenvaltion on ilman aiheetonta viivytystä poistettava kyseiset eurooppalaiset digitaalisen identiteetin lompakot käytöstä.

Jäsenvaltion on ilmoitettava asiasta asianomaisille käyttäjille, 46 c artiklan 1 kohdan mukaisesti nimetyille keskitetyille yhteyspisteille, luottaville osapuolille ja komissiolle.

2. Jos tämän artiklan 1 kohdan ensimmäisessä alakohdassa tarkoitettua tietoturvaloukkausta tai vaarantumista ei korjata kolmen kuukauden kuluessa keskeyttämisestä, jäsenvaltion, joka on tarjonnut kyseiset eurooppalaiset digitaalisen identiteetin lompakot, on poistettava kyseiset eurooppalaiset digitaalisen identiteetin lompakot käytöstä ja kumottava niiden voimassaolo. Jäsenvaltion on ilmoitettava käytöstä poistamisesta asianomaisille käyttäjille, 46 c artiklan 1 kohdan mukaisesti nimetyille keskitetyille yhteyspisteille, luottaville osapuolille ja komissiolle.
3. Kun tämän artiklan 1 kohdan ensimmäisessä alakohdassa tarkoitettu tietoturvaloukkaus tai vaarantuminen on korjattu, tarjoamisesta vastaavan jäsenvaltion on aloitettava uudelleen eurooppalaisten digitaalisen identiteetin lompakoiden tarjoaminen ja käyttö sekä ilmoitettava asiasta asianomaisille käyttäjille ja luottaville osapuolille, 46 c artiklan 1 kohdan mukaisesti nimetyille keskitetyille yhteyspisteille ja komissiolle ilman aiheetonta viivytystä.
4. Komissio julkaisee *Euroopan unionin virallisessa lehdessä* vastaavat muutokset 5 d artiklassa tarkoitettuun luetteloon ilman aiheetonta viivytystä.
5. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [kuusi kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa eritelmät ja menettelyt tämän artiklan 1, 2 ja 3 kohdassa tarkoitettuja toimenpiteitä varten antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

5 f artikla

Eurooppalaisten digitaalisen identiteetin lompakoiden rajatylittävä käyttö

1. Kun jäsenvaltio edellyttää sähköistä tunnistamista ja todentamista julkisen sektorin elimen tarjoaman verkkopalvelun käyttämiseksi, sen on hyväksyttävä myös tämän asetuksen mukaisesti tarjotut eurooppalaiset digitaalisen identiteetin lompakot.
2. Jos unionin oikeudessa tai kansallisessa lainsäädännössä edellytetään, että yksityiset luottavat osapuolet, jotka tarjoavat palveluja, lukuun ottamatta komission suosituksen 2003/361/EY^{***} liitteessä olevassa 2 artiklassa määriteltyjä mikroyrityksiä ja pieniä yrityksiä, käyttävät käyttäjän vahvaa todentamista verkossa tapahtuvaa tunnistamista varten, tai jos sopimusvelvoitteissa edellytetään käyttäjän vahvaa todentamista muun muassa liikenteen, energian, pankki- ja rahoituspalvelujen, sosiaaliturvan, terveydenhuollon, juomaveden, postipalvelujen, digitaalisen infrastruktuurin, koulutuksen tai televiestinnän aloilla, kyseisten yksityisten luottavien osapuolten on viimeistään 36 kuukauden kuluttua 5 a artiklan 23 kohdassa ja 5 c artiklan 6 kohdassa tarkoitettujen täytäntöönpanosäädösten voimaantulopäivästä ja ainoastaan käyttäjän vapaaehtoisesta pyynnöstä hyväksyttävä myös tämän asetuksen mukaisesti tarjotut eurooppalaiset digitaalisen identiteetin lompakot.
3. Jos Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2065^{****} 33 artiklassa tarkoitettujen erittäin suurten verkkoalustojen tarjoajat vaativat käyttäjien todentamista verkkopalveluihin pääsyä varten, niiden on hyväksyttävä myös tämän asetuksen mukaisesti tarjottujen eurooppalaisten digitaalisen identiteetin lompakoiden käyttö käyttäjän todentamista varten ainoastaan käyttäjän vapaaehtoisesta pyynnöstä ja niiden vähimmäistietojen osalta, jotka ovat tarpeen sen verkkopalvelun käyttämiseksi, jota varten todentamista pyydetään, ja helpotettava tällaista käyttöä.

4. Komissio helpottaa yhdessä jäsenvaltioiden kanssa käytäntöjen laatimista tiiviissä yhteistyössä kaikkien asiaankuuluvien sidosryhmien, mukaan lukien kansalaisyhteiskunta, kanssa, jotta voidaan edistää tämän asetuksen soveltamisalaan kuuluvien eurooppalaisten digitaalisen identiteetin lompakoiden laajaa saatavuutta ja käytettävyyttä sekä kannustaa palveluntarjoajia saattamaan käytäntöjen kehittäminen päätökseen.
5. Komissio arvioi 24 kuukauden kuluessa eurooppalaisten digitaalisen identiteetin lompakoiden käyttöönotosta eurooppalaisten digitaalisen identiteetin lompakoiden kysyntää, saatavuutta ja käytettävyyttä, käyttäen arviointiperusteina muun muassa käyttöönoton laajuutta käyttäjien keskuudessa, palveluntarjoajien rajatylittävää läsnäoloa, teknologian kehitystä, käyttötapojen kehittymistä ja kulutuskysyntää.

* Euroopan parlamentin ja neuvoston direktiivi (EU) 2019/882, annettu 17 päivänä huhtikuuta 2019, tuotteiden ja palvelujen esteettömyysvaatimuksista (EUVL L 151, 7.6.2019, s. 70).

** Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifiointista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus) (EUVL L 151, 7.6.2019, s. 15).

*** Komission suositus 2003/361/EY, annettu 6 päivänä toukokuuta 2003, mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä (EUVL L 124, 20.5.2003, s. 36).

**** Euroopan parlamentin ja neuvoston asetus (EU) 2022/2065, annettu 19 päivänä lokakuuta 2022, digitaalisten palvelujen sisämarkkinoista ja direktiivin 2000/31/EY muuttamisesta (digipalvelusäädös) (EUVL L 277, 27.10.2022, s. 1).”;

6) lisätään ennen 6 artiklaa otsikko seuraavasti:

”2 JAKSO

SÄHKÖISEN TUNNISTAMISEN JÄRJESTELMÄT”;

7) korvataan 7 artiklan g alakohta seuraavasti:

”g) ilmoittava jäsenvaltio toimittaa vähintään kuusi kuukautta ennen 9 artiklan 1 kohdan mukaista ilmoittamista muille jäsenvaltioille 12 artiklan 5 kohdan soveltamiseksi kuvauksen kyseisestä järjestelmästä niiden menettelytapojen mukaisesti, jotka vahvistetaan 12 artiklan 6 kohdan mukaisesti annetuissa täytäntöönpanosäädöksissä.”;

8) korvataan 8 artiklan 3 kohdan ensimmäinen alakohta seuraavasti:

”3 Ottaen huomioon asianmukaiset kansainväliset standardit ja jollei 2 kohdasta muuta johdu, komissio vahvistaa viimeistään 18 päivänä syyskuuta 2015 tekniset vähimmäiseritelmät, -standardit ja -menettelyt, joiden perusteella täsmennetään matala, korotettu ja korkea varmuustaso sähköisen tunnistamisen menetelmiä varten, antamalla täytäntöönpanosäädöksiä.”;

9) korvataan 9 artiklan 2 ja 3 kohta seuraavasti:

”2. Komissio julkaisee ilman aiheetonta viivytystä *Euroopan unionin virallisessa lehdessä* luettelon 1 kohdan nojalla ilmoitetuista sähköisen tunnistamisen järjestelmistä yhdessä niitä koskevien perustietojen kanssa.

3. Komissio julkaisee *Euroopan unionin virallisessa lehdessä* muutokset 2 kohdassa tarkoitettuun luetteloon kuukauden kuluessa asiaa koskevan ilmoituksen vastaanottamisesta.”;

10) korvataan 10 artiklan otsikko seuraavasti:

”Sähköisen tunnistamisen järjestelmien tietoturvaloukkaus”;

11) lisätään artikla seuraavasti:

”11 a artikla

Rajatyöttävä henkilöllisyyden linkittäminen

1. Toimiessaan luottavina osapuolina rajatyöttävissä palveluissa jäsenvaltioiden on varmistettava, että sellaisten luonnollisten henkilöiden henkilöllisyys, jotka käyttävät ilmoitettuja sähköisen tunnistamisen menetelmiä tai eurooppalaisia digitaalisen identiteetin lompakoita, voidaan linkittää yksiselitteisesti.
2. Jäsenvaltioiden on vahvistettava teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan henkilöllisyyden linkittämiseen käytettävien henkilötietojen korkeatasoinen suoja ja estetään käyttäjien profilointi.
3. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [kuusi kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa eritelmiä ja menettelyt tämän artiklan 1 kohdassa tarkoitettuja vaatimuksia varten antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

- 12) muutetaan 12 artikla seuraavasti:
- a) korvataan otsikko seuraavasti:
- ”Yhteentoimivuus”;
- b) muutetaan 3 kohta seuraavasti:
- i) korvataan c alakohta seuraavasti:
- ”c) sillä helpotetaan sisäänrakennetun yksityisyyden suojan ja tietoturvan soveltamista;”;
- ii) kumotaan d alakohta;
- c) korvataan 4 kohdan d alakohta seuraavasti:
- ”d) viittauksesta henkilön tunnistetietojen vähimmäismäärään, jota tarvitaan tunnistamaan yksilöivästi luonnollinen henkilö tai oikeushenkilö taikka sellainen luonnollinen henkilö, joka edustaa toista luonnollista henkilöä tai oikeushenkilöä, ja joka on saatavilla sähköisen tunnistamisen järjestelmistä;”;
- d) korvataan 5 ja 6 kohta seuraavasti:
- ”5. Jäsenvaltioiden on toteutettava vertaisarviointeja sähköisen tunnistamisen järjestelmistä, jotka kuuluvat tämän asetuksen soveltamisalaan ja joista on ilmoitettava 9 artiklan 1 kohdan a alakohdan mukaisesti.

6. Antamalla täytäntöönpanosäädöksiä komissio vahvistaa viimeistään 18 päivänä maaliskuuta 2025 tarvittavat menettelytavat tämän artiklan 5 kohdassa tarkoitettuja vertaisarviointeja varten, jotta voidaan edistää luottamuksen ja turvallisuuden korkeaa tasoa, joka on oikeassa suhteessa riskin suuruuteen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

e) poistetaan 7 kohta;

f) korvataan 8 kohta seuraavasti:

”8. Jollei tämän artiklan 3 kohdassa säädetystä perusteista muuta johdu ja ottaen huomioon jäsenvaltioiden välisen yhteistyön tulokset, komissio antaa viimeistään 18 päivänä syyskuuta 2025 täytäntöönpanosäädöksiä tämän artiklan 4 kohdassa säädetystä yhteentoimivuuskehyksestä yhdenmukaisten edellytysten asettamiseksi tämän artiklan 1 kohdan mukaisen vaatimuksen täytäntöönpanolle. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

13) lisätään II lukuun artikkelit seuraavasti:

”12 a artikla

Sähköisen tunnistamisen järjestelmien sertifiointi

1. Jäsenvaltioiden nimeämien vaatimustenmukaisuuden arviointilaitosten on sertifioitava ilmoitettavien sähköisen tunnistamisen järjestelmien vaatimustenmukaisuus tässä asetuksessa säädettyjen kyberturvallisuusvaatimusten kanssa, mukaan lukien 8 artiklan 2 kohdassa säädetty kyberturvallisuuden kannalta merkitykselliset vaatimukset, jotka koskevat sähköisen tunnistamisen järjestelmien varmuustasoja.
2. Tämän artiklan 1 kohdan mukainen sertifiointi on tehtävä asetuksen (EU) 2019/881 mukaisen asiaankuuluvan kyberturvallisuuden sertifiointijärjestelmän tai sen osien mukaisesti siltä osin kuin kyberturvallisuussertifikaatti tai sen osat kattavat kyseiset kyberturvallisuusvaatimukset.
3. Edellä olevan 1 kohdan mukainen sertifiointi on voimassa enintään viisi vuotta edellyttäen, että haavoittuvuusarviointi tehdään joka toinen vuosi. Jos haavoittuvuus havaitaan eikä sitä korjata kolmen kuukauden kuluessa havaitsemisesta, sertifiointi peruutetaan.
4. Sen estämättä, mitä 2 kohdassa säädetään, jäsenvaltiot voivat kyseisen kohdan mukaisesti pyytää ilmoittavalta jäsenvaltiolta lisätietoja sertifioiduista sähköisen tunnistamisen järjestelmistä tai niiden osista.

5. Jäljempänä 12 artiklan 5 kohdassa tarkoitettua sähköisen tunnistamisen järjestelmien vertaisarviointia ei sovelleta tämän artiklan 1 kohdan mukaisesti sertifioituihin sähköisen tunnistamisen järjestelmiin tai niiden osiin. Jäsenvaltiot voivat käyttää asiaankuuluvien sertifiointijärjestelmien tai niiden osien mukaisesti myönnettyä sertifikaattia tai vaatimustenmukaisuusilmoitusta osoittaakseen, että tällaiset järjestelmät ovat 8 artiklan 2 kohdassa säädettyjen sähköisen tunnistamisen järjestelmien varmuustasoa koskevien, muiden kuin kyberturvallisuuteen liittyvien vaatimusten mukaisia.
6. Jäsenvaltioiden on ilmoitettava komissiolle 1 kohdassa tarkoitettujen vaatimustenmukaisuuden arviointilaitosten nimet ja osoitteet. Komissio asettaa nämä tiedot kaikkien jäsenvaltioiden saataville.

12 b artikla

Pääsy laitteisto- ja ohjelmisto-ominaisuuksiin

Jos eurooppalaisten digitaalisen identiteetin lompakoiden tarjoajat ja ilmoitettujen sähköisen tunnistamisen menetelmien myöntäjät, jotka toimivat kaupallisessa tai ammatillisessa ominaisuudessa ja käyttävät Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/1925* 2 artiklan 2 kohdassa määriteltyjä ydinalustapalveluja eurooppalaisen digitaalisen identiteetin lompakon palvelujen ja sähköisen tunnistamisen menetelmien loppukäyttäjille tarjoamista varten tai tarjoamisen aikana, ovat mainitun asetuksen 2 artiklan 21 kohdan mukaisia yrityskäyttäjiä, portinvartijoiden on erityisesti mahdollistettava niiden tehokas yhteentoimivuus saman käyttöjärjestelmän tai laitteisto- tai ohjelmisto-ominaisuuksien kanssa ja pääsy niihin yhteentoimivuuden varmistamiseksi. Tällainen tehokas yhteentoimivuus ja pääsy on sallittava maksutta riippumatta siitä, ovatko laitteisto- tai ohjelmisto-ominaisuudet osa käyttöjärjestelmää, sellaisena kuin ne ovat kyseisen portinvartijan saatavilla tai sellaisena kuin se niitä käyttää tarjotessaan tällaisia palveluja asetuksen (EU) 2022/1925 6 artiklan 7 kohdassa tarkoitetulla tavalla. Tämä artikla ei rajoita tämän asetuksen 5 a artiklan 14 kohdan soveltamista.

* Euroopan parlamentin ja neuvoston asetus (EU) 2022/1925, annettu 14 päivänä syyskuuta 2022, kilpailullisista ja oikeudenmukaisista markkinoista digitaalisella ja digitaalialalla ja direktiivien (EU) 2019/1937 ja (EU) 2020/1828 muuttamisesta (digimarkkinasäädös) (EUVL L 265, 12.10.2022, s. 1).”;

14) korvataan 13 artiklan 1 kohta seuraavasti:

”1. Sen estämättä, mitä tämän artiklan 2 kohdassa säädetään, ja rajoittamatta asetuksen (EU) 2016/679 soveltamista, luottamuspalvelun tarjoajat ovat vastuussa luonnolliselle henkilölle tai oikeushenkilölle tahallaan tai tuottamuksesta aiheutetusta vahingosta, joka johtuu tämän asetuksen mukaisten velvoitteiden noudattamatta jättämisestä. Jokaisella luonnollisella henkilöllä tai oikeushenkilöllä, jolle on aiheutunut aineellista tai aineetonta vahinkoa siitä, että luottamuspalvelun tarjoaja on rikkonut tätä asetusta, on oikeus hakea korvausta unionin oikeuden ja kansallisen lainsäädännön mukaisesti.

Ei-hyväksytyn luottamuspalvelujen tarjoajan tahallisuutta tai tuottamuksellisuutta koskeva todistustaakka on luonnollisella henkilöllä tai oikeushenkilöllä, joka hakee korvausta ensimmäisessä alakohdassa tarkoitettua vahingosta.

Hyväksytyn luottamuspalvelun tarjoajan oletetaan ensimmäisessä alakohdassa tarkoitettua vahingon osalta toimineen tahallaan tai tuottamuksesta, ellei kyseinen hyväksytty luottamuspalvelun tarjoaja toisin osoita.”;

15) korvataan 14, 15 ja 16 artikla seuraavasti:

”14 artikla

Kansainväliset näkökohdat

1. Kolmanteen maahan sijoittautuneiden luottamuspalvelun tarjoajien tai kansainvälisten järjestöjen tarjoamat luottamuspalvelut on tunnustettava oikeusvaikutuksiltaan vastaaviksi kuin unionin alueelle sijoittautuneiden hyväksytyjen luottamuspalvelun tarjoajien tarjoamat hyväksytyt luottamuspalvelut, jos kolmannelle maasta tai kansainvälisestä järjestöstä lähtöisin olevat luottamuspalvelut tunnustetaan täytäntöönpanosäädöksessä tai Euroopan unionin toiminnasta tehdyn sopimuksen 218 artiklan mukaisesti unionin ja kolmannen maan tai kansainvälisen järjestön välillä tehdyssä sopimuksessa.

Ensimmäisessä alakohdassa tarkoitettua täytäntöönpanosäädöksiä hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

2. Edellä 1 kohdassa tarkoitetuilla täytäntöönpanosäädöksillä ja sopimuksella on varmistettava, että kyseisessä kolmannessa maassa toimivat luottamuspalvelun tarjoajat tai kansainväliset järjestöt ja niiden tarjoamat luottamuspalvelut täyttävät unionin alueelle sijoittautuneisiin hyväksytyihin luottamuspalvelun tarjoajiin ja niiden tarjoamiin hyväksytyihin luottamuspalveluihin sovellettavat vaatimukset. Kolmansien maiden ja kansainvälisten järjestöjen on erityisesti laadittava ja julkaistava luotettu luettelo tunnustetuista luottamuspalvelun tarjoajista ja ylläpidettävä sitä.

3. Edellä 1 kohdassa tarkoitetuilla sopimuksilla on varmistettava, että unionin alueelle sijoittautuneiden hyväksytyjen luottamuspalvelun tarjoajien tarjoamat hyväksytyt luottamuspalvelut tunnustetaan oikeusvaikutuksiltaan vastaaviksi kuin sellaisessa kolmannessa maassa toimivien luottamuspalvelun tarjoajien tai sellaisen kansainvälisen järjestön, jonka kanssa sopimus tehdään, tarjoamat luottamuspalvelut.

15 artikla

Esteettömyys vammaisten ja erityistarpeisten henkilöiden näkökulmasta

Sähköisen tunnistamisen menetelmät, luottamuspalvelut ja loppukäyttäjätuotteet, joita käytetään kyseisten palvelujen tarjoamisessa, on tarjottava saataville selkeällä ja ymmärrettävällä kielellä vammaisten henkilöiden oikeuksia koskevan Yhdistyneiden kansakuntien yleissopimuksen ja direktiivin (EU) 2019/882 esteettömyysvaatimusten mukaisesti, mikä hyödyttää myös toimintarajoitteisia henkilöitä, kuten ikääntyneitä henkilöitä, ja henkilöitä, joilla on rajalliset mahdollisuudet käyttää digitaaliteknologiaa.

16 artikla

Seuraamukset

1. Jäsenvaltioiden on säädettävä säännöistä, jotka koskevat tämän asetuksen rikkomiseen sovellettavia seuraamuksia, sanotun kuitenkin rajoittamatta Euroopan parlamentin ja direktiivin (EU) 2022/2555* 31 artiklan soveltamista. Kyseisten seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia.

2. Jäsenvaltioiden on varmistettava, että jos hyväksytyt ja ei-hyväksytyt luottamuspalvelun tarjoajat rikkovat tätä asetusta, niille määrätään hallinnollinen sakko, jonka enimmäismäärä on vähintään
- a) 5 000 000 euroa, jos luottamuspalvelun tarjoaja on luonnollinen henkilö; tai
 - b) 5 000 000 euroa tai yksi prosentti sen yrityksen maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta, johon luottamuspalvelun tarjoaja kuului rikkomisvuotta edeltävänä tilikautena, sen mukaan, kumpi näistä määristä on suurempi, jos luottamuspalvelun tarjoaja on oikeushenkilö.
3. Jäsenvaltion oikeusjärjestelmästä riippuen hallinnollisia sakkoja koskevia sääntöjä voidaan soveltaa siten, että sakkojen määräämistä ehdottava toimivaltainen valvontaelin ja määräämisestä vastaavat toimivaltaiset kansalliset tuomioistuimet. Tällaisten sääntöjen soveltamisella kyseisissä jäsenvaltioissa on varmistettava, että kyseiset oikeussuojakeinot ovat tehokkaita ja niillä on vastaava vaikutus kuin valvontaviranomaisten suoraan määräämillä hallinnollisilla sakoilla.

* Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi) (EUVL L 333, 27.12.2022, s. 80).”;

16) korvataan III luvun 2 jakson otsikko seuraavasti:

”Ei-hyväksytyt luottamuspalvelut”;

17) kumotaan 17 ja 18 artikla;

18) lisätään III luvun 2 jaksoon artikla seuraavasti:

”19 a artikla

Ei-hyväksytyjä luottamuspalvelun tarjoajia koskevat vaatimukset

1. Ei-hyväksytyjä luottamuspalveluja tarjoavan ei-hyväksytyin luottamuspalvelun tarjoajan on

- a) noudatettava asianmukaisia toimintaperiaatteita ja toteutettava ei-hyväksytyjen luottamuspalvelujen tarjoamiseen kohdistuvien oikeudellisten, liiketoiminnallisten, operatiivisten ja muiden suorien tai välillisten riskien hallitsemiseksi vastaavat toimenpiteet, joihin on sen estämättä, mitä direktiivin (EU) 2022/2555 21 artiklassa säädetään, sisällyttävä vähintään seuraavia koskevat toimenpiteet:
 - i) luottamuspalveluun rekisteröityminen ja käyttösuhteen aloittamismenettelyt;
 - ii) luottamuspalvelujen tarjoamiseen tarvittavat menettelylliset tai hallinnolliset tarkastukset;
 - iii) luottamuspalvelujen hallinnointi ja toteuttaminen;

b) ilmoitettava valvontaelimelle, tunnistettavissa oleville asianomaisille henkilöille, yleisölle, jos se on yleisen edun mukaista, ja tarvittaessa muille asiaankuuluville toimivaltaisille viranomaisille ilman aiheetonta viivytystä ja joka tapauksessa viimeistään 24 tunnin kuluttua siitä, kun ne ovat tulleet asiasta tietoisiksi, kaikista tietoturvaloukkauksista tai palvelujen tarjoamisen tai a alakohdan i, ii ja iii alakohdassa tarkoitettujen toimenpiteiden häiriöistä, joilla on merkittävä vaikutus tarjottuun luottamuspalveluun tai siinä säilytettyihin henkilötietoihin.

2. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa tämän artiklan 1 kohdan a alakohtaa koskevat eritelmät ja menettelyt antamalla täytäntöönpanosäädöksiä. Jos näitä standardeja, teknisiä eritelmiä ja menettelyjä noudatetaan, tässä artiklassa säädettyjen vaatimusten katsotaan täyttyvän. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

19) muutetaan 20 artikla seuraavasti:

a) korvataan 1 kohta seuraavasti:

”1. Vaatimustenmukaisuuden arviointilaitoksen on tarkastettava hyväksytyt luottamuspalvelun tarjoajat vähintään 24 kuukauden välein niiden omalla kustannuksella. Tarkastuksen on vahvistettava, että hyväksytyt luottamuspalvelun tarjoajat ja niiden tarjoamat hyväksytyt luottamuspalvelut täyttävät tässä asetuksessa ja direktiivin (EU) 2022/2555 21 artiklassa säädetyt vaatimukset. Hyväksytyjen luottamuspalvelun tarjoajien on toimitettava tarkastuksen perusteella laadittava vaatimustenmukaisuuden arviointikertomus valvontaelimelle kolmen työpäivän kuluessa sen vastaanottamisesta.”;

b) lisätään kohdat seuraavasti:

”1 a. Hyväksytyjen luottamuspalvelun tarjoajien on ilmoitettava valvontaelimelle viimeistään kuukautta etukäteen suunnitelluista tarkastuksista ja sallittava pyynnöstä valvontaelimen osallistuminen tarkkailijana.

1 b. Jäsenvaltioiden on ilman aiheetonta viivytystä ilmoitettava komissiolle 1 kohdassa tarkoitettujen vaatimustenmukaisuuden arviointilaitosten nimet, osoitteet ja akkreditointitiedot ja niiden mahdolliset myöhemmät muutokset. Komissio asettaa nämä tiedot kaikkien jäsenvaltioiden saataville.”;

c) korvataan 2, 3 ja 4 kohta seuraavasti:

”2. Valvontaelin voi milloin tahansa tehdä hyväksytyille luottamuspalvelun tarjoajille tarkastuksia tai pyytää vaatimustenmukaisuuden arviointilaitosta suorittamaan hyväksytyjä luottamuspalvelun tarjoajia koskevan vaatimustenmukaisuuden arvioinnin näiden hyväksytyjen luottamuspalvelun tarjoajien kustannuksella sen vahvistamiseksi, että ne ja niiden tarjoamat hyväksytyt luottamuspalvelut täyttävät tässä asetuksessa säädetyt vaatimukset, sanotun kuitenkin rajoittamatta 1 kohdan soveltamista. Jos näyttää siltä, että henkilötietojen suojaan liittyviä sääntöjä on rikottu, valvontaelimen on ilman aiheetonta viivytystä ilmoitettava siitä asetuksen (EU) 2016/679 51 artiklan nojalla perustetuille toimivaltaisille valvontaviranomaisille.

3. Jos hyväksytty luottamuspalvelun tarjoaja ei täytä jotain tässä asetuksessa säädetyistä vaatimuksista, valvontaelimen on vaadittava sitä korjaamaan asia tarvittaessa tietyn määräajan kuluessa.

Jos kyseinen palveluntarjoaja ei korjaa asiaa tai tapauksen mukaan ei tee sitä valvontaelimen asettamassa määräajassa, valvontaelimen on, kun se on perusteltua erityisesti laiminlyönnin laajuuden, keston ja seurausten perusteella, peruttava kyseisen palveluntarjoajan tai sen tarjoaman kyseessä olevan palvelun hyväksytty asema.

- 3 a. Jos direktiivin (EU) 2022/2555 8 artiklan 1 kohdan nojalla nimetyt tai perustetut toimivaltaiset viranomaiset ilmoittavat valvontaelimelle, että hyväksytty luottamuspalvelun tarjoaja ei täytä jotain kyseisen direktiivin 21 artiklassa säädetyistä vaatimuksista, valvontaelimen on, kun se on perusteltua erityisesti laiminlyönnin laajuuden, keston ja seurausten perusteella, peruttava kyseisen palveluntarjoajan tai sen tarjoaman kyseessä olevan palvelun hyväksytty asema.

- 3 b. Jos asetuksen (EU) 2016/679 51 artiklan nojalla perustetut valvontaviranomaiset ilmoittavat valvontaelimelle, että hyväksytty luottamuspalvelun tarjoaja ei täytä jotain kyseisessä asetuksessa säädetyistä vaatimuksista, valvontaelimen on, kun se on perusteltua erityisesti laiminlyönnin laajuuden, keston ja seurausten perusteella, peruttava kyseisen palveluntarjoajan tai sen tarjoaman kyseessä olevan palvelun hyväksytty asema.

- 3 c. Valvontaelimen on ilmoitettava hyväksytylle luottamuspalvelun tarjoajalle sen hyväksytyin aseman tai kyseessä olevan palvelun hyväksytyin aseman perumisesta. Valvontaelimen on ilmoitettava asiasta tämän asetuksen 22 artiklan 3 kohdan mukaisesti ilmoitetulle elimelle kyseisen artiklan 1 kohdassa tarkoitettujen luotettujen luetteloiden päivittämiseksi ja direktiivin (EU) 2022/2555 8 artiklan 1 kohdan nojalla nimetyille tai perustetuille toimivaltaiselle viranomaiselle.
4. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] täytäntöönpanosäädöksin luettelon viitestandardeista ja tarvittaessa eritelvät ja menettelyt seuraavia varten:
- a) 1 kohdassa tarkoitettu vaatimustenmukaisuuden arviointilaitosten akkreditointi ja vaatimustenmukaisuuden arviointikertomus;
 - b) tarkastusvaatimukset, joiden mukaisesti vaatimustenmukaisuuden arviointilaitokset suorittavat 1 kohdassa tarkoitettujen hyväksytyjen luottamuspalvelun tarjoajien vaatimustenmukaisuuden arvioinnin, mukaan lukien yhdistetyn arvioinnin;
 - c) vaatimustenmukaisuuden arviointijärjestelmät, joiden mukaisesti vaatimustenmukaisuuden arviointilaitokset suorittavat hyväksytyjen luottamuspalvelujen tarjoajien vaatimustenmukaisuuden arvioinnin ja antavat 1 kohdassa tarkoitettua raportin.

Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

20) muutetaan 21 artikla seuraavasti:

a) korvataan 1 ja 2 kohta seuraavasti:

- ”1. Jos luottamuspalvelun tarjoajat aikovat aloittaa hyväksytyt luottamuspalvelun tarjoamisen, niiden on ilmoitettava valvontaelimelle aikeestaan ja yhdessä sen kanssa vaatimustenmukaisuuden arviointilaitoksen antama vaatimustenmukaisuuden arviointiraportti, jossa vahvistetaan tässä asetuksessa ja direktiivin (EU) 2022/2555 21 artiklassa säädettyjen vaatimusten täytyminen.
2. Valvontaelimen on tarkastettava, täyttävätkö luottamuspalvelun tarjoaja ja sen tarjoamat luottamuspalvelut tässä asetuksessa säädetyt vaatimukset ja erityisesti hyväksytyt luottamuspalvelun tarjoajia ja niiden tarjoamia hyväksytyt luottamuspalveluja koskevat vaatimukset.

Sen tarkastamiseksi, että luottamuspalvelun tarjoaja noudattaa direktiivin (EU) 2022/2555 21 artiklassa säädettyjä vaatimuksia, valvontaelimen on pyydettävä kyseisen direktiivin 8 artiklan 1 kohdan nojalla nimettyjä tai perustettuja toimivaltaisia viranomaisia toteuttamaan tältä osin valvontatoimia ja toimittamaan tiedot toimien tuloksista ilman aiheetonta viivytystä ja joka tapauksessa kahden kuukauden kuluessa pyynnön vastaanottamisesta. Jos tarkastusta ei saada päätökseen kahden kuukauden kuluessa ilmoituksesta, kyseisten toimivaltaisten viranomaisten on ilmoitettava asiasta valvontaelimelle ja yksilöitävä viivästyksen syyt ja ajanjakso, jonka aikana tarkastus on määrä saada päätökseen.

Jos valvontaelin katsoo, että luottamuspalvelun tarjoaja ja sen tarjoamat luottamuspalvelut täyttävät tässä asetuksessa säädetyt vaatimukset, valvontaelimen on myönnettävä luottamuspalvelun tarjoajalle ja sen tarjoamille luottamuspalveluille hyväksytyt asema sekä ilmoitettava asiasta 22 artiklan 3 kohdassa tarkoitettulle elimelle 22 artiklan 1 kohdassa tarkoitettujen luotettujen luetteloiden ajan tasalle saattamista varten viimeistään kolmen kuukauden kuluttua tämän artiklan 1 kohdan mukaisesta ilmoituksesta.

Jos tarkastusta ei saada päätökseen kolmen kuukauden kuluessa ilmoituksesta, valvontaelimen on ilmoitettava asiasta luottamuspalvelun tarjoajalle ja yksilöitävä viivästyksen syyt ja ajanjakso, jonka aikana tarkastus on määrä saada päätökseen.”;

b) korvataan 4 kohta seuraavasti:

”4. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] tämän artiklan 1 ja 2 kohdan soveltamiseksi tehtäviin ilmoituksiin ja tarkastuksiin liittyvät muotoseikat ja menettelyt antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

21) muutetaan 24 artikla seuraavasti:

a) korvataan 1 kohta seuraavasti:

”1. Kun hyväksytty luottamuspalvelun tarjoaja myöntää hyväksytyn varmenteen tai hyväksytyn sähköisen attribuuttitodistuksen, sen on tarkastettava sen luonnollisen tai oikeushenkilön henkilöllisyys ja mahdolliset muut attribuutit, jolle hyväksytty varmenne tai hyväksytty sähköinen attribuuttitodistus myönnetään.

1 a. Hyväksytyn luottamuspalvelun tarjoajan on tarkastettava 1 kohdassa tarkoitettu henkilöllisyys asianmukaisin keinoin joko suoraan tai kolmannen osapuolen avulla perustuen tarvittaessa johonkin seuraavista menetelmistä tai niiden yhdistelmään 1 c kohdassa tarkoitettujen täytäntöönpanosäädösten mukaisesti:

- a) käyttäen eurooppalaista digitaalisen identiteetin lompakkoa tai ilmoitettua sähköisen tunnistamisen menetelmää, joka täyttää 8 artiklassa säädetyt korkea varmuustasoa koskevat vaatimukset;
- b) käyttäen a, c tai d alakohdan mukaisesti myönnettyä hyväksytyn sähköisen allekirjoituksen tai hyväksytyn sähköisen leiman varmennetta;
- c) käyttäen muita tunnistamismenetelmiä, jotka takaavat henkilön tunnistamisen korkealla luottamustasolla ja joiden vaatimustenmukaisuuden vahvistaa vaatimustenmukaisuuden arviointilaitos;

d) luonnollisen henkilön tai oikeushenkilön valtuutetun edustajan fyysisellä läsnäololla, käyttäen asianmukaisia todisteita ja menettelyjä kansallisen lainsäädännön mukaisesti.

1 b. Hyväksytyin luottamuspalvelun tarjoajan on tarkastettava 1 alakohdassa tarkoitetut attribuutit asianmukaisin keinoin joko suoraan tai kolmannen osapuolen avulla perustuen johonkin seuraavista menetelmistä tai tarvittaessa niiden yhdistelmään 1 c kohdassa tarkoitettujen täytäntöönpanosäädösten mukaisesti:

- a) käyttäen eurooppalaista digitaalisen identiteetin lompakkoa tai ilmoitettua sähköisen tunnistamisen menetelmää, joka täyttää 8 artiklassa säädetyt korkea varmuustasoa koskevat vaatimukset;
- b) käyttäen 1 a kohdan a, c tai d alakohdan mukaisesti myönnettyä hyväksytyin sähköisen allekirjoituksen tai hyväksytyin sähköisen leiman varmennetta;
- c) käyttäen hyväksytyin sähköistä attribuuttitodistusta;
- d) käyttäen muita menetelmiä, jotka takaavat attribuuttien todentamisen korkealla luottamustasolla ja joiden vaatimustenmukaisuuden vahvistaa vaatimustenmukaisuuden arviointilaitos;

- e) luonnollisen henkilön tai oikeushenkilön valtuutetun edustajan fyysisen läsnäolon avulla, käyttäen asianmukaisia todisteita ja menettelyjä kansallisen lainsäädännön mukaisesti.
- 1 c. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] täytäntöönpanosäädöksiin luettelon viitestandardeista ja tarvittaessa eritelvät ja menettelyt tämän artiklan 1, 1 a ja 1 b kohdassa tarkoitettujen henkilöllisyyden ja attribuuttien tarkastamista varten. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen. ”;
- b) muutetaan 2 kohta seuraavasti:
 - i) korvataan a alakohta seuraavasti:
 - ”a) ilmoitettava valvontaelimelle vähintään kuukautta aikaisemmin, ennen kuin se toteuttaa muutoksia hyväksytyjen luottamuspalvelujensa tarjoamiseen, tai vähintään kolme kuukautta aikaisemmin, jos tarkoituksena on lopettaa kyseinen toiminta;”;
 - ii) korvataan d ja e alakohta seuraavasti:
 - ”d) ilmoitettava ennen sopimussuhteen aloittamista julkisesti käytettävissä olevassa tilassa ja henkilökohtaisesti henkilöille, jotka haluavat käyttää hyväksytyä luottamuspalvelua, selkeästi, kattavasti ja helposti saatavilla olevassa muodossa kyseisen palvelun käytön tarkoista ehdoista ja edellytyksistä, muun muassa sen käyttöä koskevista rajoituksista;

- e) käytettävä luotettavia järjestelmiä ja tuotteita, jotka on suojattu muutoksilta ja joilla varmistetaan niiden tukemien prosessien tekninen tietoturva ja luotettavuus, mukaan lukien soveltuvien salaustekniikoiden käyttö;”;
- iii) lisätään alakohdat seuraavasti:
 - ”f a) sen estämättä, mitä direktiivin (EU) 2022/2555 21 artiklassa säädetään, noudatettava asianmukaisia toimintaperiaatteita ja toteutettava vastaavat toimenpiteet hyväksytyjen luottamuspalvelujen tarjoamiseen kohdistuvien oikeudellisten, liiketoiminnallisten, operatiivisten ja muiden suorien tai välillisten riskien hallitsemiseksi, mukaan lukien vähintään seuraavia koskevat toimenpiteet:
 - i) palveluun rekisteröityminen ja käyttösuhteen aloittamismenettelyt;
 - ii) menettelylliset tai hallinnolliset tarkastukset;
 - iii) palvelujen hallinnointi ja toteuttaminen;
 - f b) ilmoitettava valvontaelimelle, tunnistettavissa oleville asianomaisille henkilöille, tarvittaessa muille asiaankuuluville toimivaltaisille elimille sekä valvontaelimen pyynnöstä yleisölle, jos se on yleisen edun mukaista, ilman aiheetonta viivytystä ja joka tapauksessa viimeistään 24 tunnin kuluttua poikkeamasta palvelujen tarjoamisessa tai f a alakohdan i, ii tai iii alakohdassa tarkoitettujen toimenpiteiden toteuttamisessa havaituista tietoturvaloukkauksista tai häiriöistä, joilla on merkittävä vaikutus tarjottuun luottamuspalveluun tai siinä säilytettyihin henkilötietoihin;”;

iv) korvataan g, h ja i alakohta seuraavasti:

”g) toteutettava tarkoituksenmukaisia toimenpiteitä tietojen väärentämisen, varastamisen tai väärinkäytön tai niiden oikeudettoman tuhoamisen, muuttamisen tai käyttökelvottomaksi tekemisen estämiseksi;

h) arkistoitava ja pidettävä saatavilla niin kauan kuin tarpeellista sen jälkeen, kun hyväksytyn luottamuspalvelun tarjoajan toiminta on lakannut, kaikki tarvittavat tiedot hyväksytyn luottamuspalvelun tarjoajan myöntämistä ja vastaanottamista tiedoista, jotta niitä voidaan käyttää todisteena oikeudellisissa käsittelyissä ja jotta voidaan varmistaa palvelun jatkuvuus. Tällaisia arkistoja voidaan ylläpitää sähköisessä muodossa;

i) ylläpidettävä ajan tasalla olevaa toiminnan lopettamissuunnitelmaa, jotta voidaan varmistaa palvelun jatkuvuus valvontaelimen 46 b artiklan 4 kohdan i alakohdan nojalla tarkastamien säännösten mukaisesti;”;

v) kumotaan j alakohta;

vi) lisätään alakohta seuraavasti:

”Valvontaelin voi pyytää lisätietoja ensimmäisen kohdan a alakohdan nojalla ilmoitettujen tietojen lisäksi tai vaatimustenmukaisuuden arvioinnin tuloksen, ja se voi asettaa luvan myöntämisen ehdoksi, että suunnitellut muutokset hyväksytyihin luottamuspalveluihin toteutetaan. Jos tarkastusta ei saada päätökseen kolmen kuukauden kuluessa ilmoituksesta, valvontaelimen on ilmoitettava asiasta luottamuspalvelun tarjoajalle ja yksilöitävä viivästyksen syyt ja ajanjakso, jonka aikana tarkastus on määrä saada päätökseen.”;

c) korvataan 5 kohta seuraavasti:

”4 a. Edellä olevaa 3 ja 4 kohtaa sovelletaan vastaavasti hyväksytyjen sähköisten attribuuttitodistusten peruuttamiseen.

4 b. Siirretään komissiolle valta antaa 47 artiklan mukaisesti delegoituja säädöksiä, joilla vahvistetaan tämän artiklan 2 kohdan f a alakohdassa tarkoitettuja lisätoimenpiteitä.

5. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa tämän artiklan 2 kohdassa tarkoitettuja vaatimuksia koskevat eritelmät ja menettelyt antamalla täytäntöönpanosäädöksiä. Jos näitä standardeja, teknisiä eritelmiä ja menettelyjä noudatetaan, tässä kohdassa säädettyjen vaatimusten katsotaan täyttyvän. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

22) lisätään III luvun 3 jaksoon artikla seuraavasti:

”24 a artikla

Hyväksytyjen luottamuspalvelujen tunnustaminen

1. Missä tahansa jäsenvaltiossa myönnetyt hyväksytyihin varmenteisiin perustuvat hyväksytyt sähköiset allekirjoitukset ja missä tahansa jäsenvaltiossa myönnettyyn hyväksytyyn varmenteeseen perustuvat hyväksytyt sähköiset leimat on kaikissa muissa jäsenvaltioissa tunnustettava hyväksytyiksi sähköisiksi allekirjoituksiksi ja hyväksytyiksi sähköisiksi leimoiksi.
2. Hyväksytyt sähköisen allekirjoituksen luontivälineet ja missä tahansa jäsenvaltiossa sertifioidut hyväksytyt sähköisen leiman luontivälineet on kaikissa muissa jäsenvaltioissa tunnustettava hyväksytyiksi sähköisen allekirjoituksen luontivälineiksi ja hyväksytyiksi sähköisen leiman luontivälineiksi.
3. Missä tahansa jäsenvaltiossa toimitetut sähköisten allekirjoitusten hyväksytyt varmenteet, sähköisten leimojen hyväksytyt varmenteet, hyväksytyt luottamuspalvelut hyväksytyjen sähköisen allekirjoituksen etäluontivälineiden hallinnointia varten ja hyväksytyjen sähköisen leiman etäluontivälineiden hallinnoinnin hyväksytyt palvelut on kaikissa muissa jäsenvaltioissa tunnustettava sähköisten allekirjoitusten hyväksytyiksi varmenteiksi, sähköisten leimojen hyväksytyiksi varmenteiksi, hyväksytyiksi luottamuspalveluiksi hyväksytyjen sähköisen allekirjoituksen etäluontivälineiden hallinnointia varten ja hyväksytyjen sähköisen leiman etäluontivälineiden hallinnoinnin hyväksytyiksi palveluiksi.

4. Missä tahansa jäsenvaltiossa tarjottavat hyväksytyjen sähköisten allekirjoitusten hyväksytyt validointipalvelut ja hyväksytyjen sähköisten leimojen hyväksytyt validointipalvelut on kaikissa muissa jäsenvaltioissa tunnustettava hyväksytyjen sähköisten allekirjoitusten hyväksytyiksi validointipalveluiksi ja hyväksytyjen sähköisten leimojen hyväksytyiksi validointipalveluiksi.
5. Missä tahansa jäsenvaltiossa tarjottavat hyväksytyjen sähköisten allekirjoitusten hyväksytyt säilyttämispalvelut ja hyväksytyjen sähköisten leimojen hyväksytyt säilyttämispalvelut on kaikissa muissa jäsenvaltioissa tunnustettava hyväksytyjen sähköisten allekirjoitusten hyväksytyiksi säilyttämispalveluiksi ja hyväksytyjen sähköisten leimojen hyväksytyiksi säilyttämispalveluiksi.
6. Missä tahansa jäsenvaltiossa toimitettu hyväksytty sähköinen aikaleima on kaikissa muissa jäsenvaltioissa tunnustettava hyväksytyksi sähköiseksi aikaleimaksi.
7. Missä tahansa jäsenvaltiossa myönnetty verkkosivustojen todentamisen hyväksytty varmenne on kaikissa muissa jäsenvaltioissa tunnustettava verkkosivustojen todentamisen hyväksytyksi varmenteeksi.
8. Missä tahansa jäsenvaltiossa tarjottava hyväksytty sähköinen rekisteröity jakelupalvelu on kaikissa muissa jäsenvaltioissa tunnustettava hyväksytyksi sähköiseksi rekisteröidyksi jakelupalveluksi.
9. Missä tahansa jäsenvaltiossa myönnetty hyväksytty sähköinen attribuuttitodistus on kaikissa muissa jäsenvaltioissa tunnustettava hyväksytyksi sähköiseksi attribuuttitodistukseksi.

10. Missä tahansa jäsenvaltiossa tarjottava hyväksytty sähköinen arkistointipalvelu on kaikissa muissa jäsenvaltioissa tunnustettava hyväksytyksi sähköiseksi arkistointipalveluksi.

11. Missä tahansa jäsenvaltiossa toimitettu hyväksytty sähköinen tilikirja on kaikissa muissa jäsenvaltioissa tunnustettava hyväksytyksi sähköiseksi tilikirjaksi.”;

23) kumotaan 25 artiklan 3 kohta;

24) muutetaan 26 artikla seuraavasti:

a) ainoasta kohdasta tulee 1 kohta;

b) lisätään kohta seuraavasti:

”2. Komissio arvioi viimeistään ... päivänä ...kuuta ... [24 kuukauden kuluttua tämän muutosasetuksen voimaantulopäivästä], onko tarpeen antaa täytäntöönpanosäädöksiä, joissa vahvistetaan luettelo viitestandardeista ja tarvittaessa kehittyneitä sähköisiä allekirjoituksia koskevat eritelmät ja menettelyt. Komissio voi kyseisen arvioinnin perusteella antaa tällaisia täytäntöönpanosäädöksiä. Kehittyneitä sähköisiä allekirjoituksia koskevien vaatimusten katsotaan täyttyvän, kun kehittynyt sähköinen allekirjoitus on kyseisten standardien, eritelmien ja menettelyjen mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

25) kumotaan 27 artiklan 4 kohta;

26) korvataan 28 artiklan 6 kohta seuraavasti:

”6. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa sähköisen allekirjoituksen hyväksytyihin varmenteisiin sovellettavat eritelvät ja menettelyt antamalla täytäntöönpanosäädöksiä. Jos sähköisen allekirjoituksen hyväksyty varmenne vastaa kyseisiä standardeja, eritelmiä ja menettelyjä, sen katsotaan olevan liitteessä I säädettyjen vaatimusten mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

27) lisätään 29 artiklaan kohta seuraavasti:

”1 a. Sähköisen allekirjoituksen luontitietojen muodostaminen tai hallinnointi tai tällaisten sähköisen allekirjoituksen luontitietojen kahdentaminen varmuuskopiointitarkoituksiin voidaan suorittaa vain allekirjoittajan puolesta ja allekirjoittajan pyynnöstä ja tällaisesta muodostamisesta tai hallinnoinnista tai kahdentamisesta saa vastata ainoastaan hyväksyty luottamuspalvelun tarjoaja, joka tarjoaa hyväksytyä luottamuspalvelua hyväksytyn sähköisen allekirjoituksen etäluontivälineen hallinnointia varten.”;

28) lisätään artikla seuraavasti:

”29 a artikla

*Hyväksytyjen sähköisen allekirjoituksen etäluontivälineiden
hallinnoinnin hyväksytyä palvelua koskevat vaatimukset*

1. Hyväksytyn sähköisen allekirjoituksen etäluontivälineen hallinnoinnista hyväksyttynä palveluna saa vastata ainoastaan hyväksyty luottamuspalvelun tarjoaja, joka
 - a) muodostaa tai hallinnoi sähköisen allekirjoituksen luontitietoja allekirjoittajan puolesta;
 - b) sen estämättä, mitä liitteessä II olevan 1 kohdan d alakohdassa säädetään, kahdentaa sähköisen allekirjoituksen luontitietoja ainoastaan varmuuskopiointitarkoituksiin edellyttäen, että seuraavat vaatimukset täyttyvät:
 - i) kahdennettujen tietokokonaisuuksien tietoturvan on oltava samalla tasolla kuin alkuperäisten tietokokonaisuuksien;
 - ii) kahdennettujen tietokokonaisuuksien määrä ei saa ylittää vähimmäismäärää, joka on tarpeen palvelun jatkuvuuden varmistamiseksi;
 - c) täyttää kaikki 30 artiklan nojalla annetussa yksittäisen hyväksytyn sähköisen allekirjoituksen etäluontivälineen sertifiointiraportissa määritetyt vaatimukset.

2. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa tämän artiklan 1 kohdan soveltamiseen liittyvät eritelvät ja menettelyt antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

29) lisätään 30 artiklaan kohta seuraavasti:

”3 a. Edellä 1 kohdassa tarkoitettu sertifiointi on voimassa enintään viisi vuotta edellyttäen, että haavoittuvuuksia arvioidaan kahden vuoden välein. Jos haavoittuvuuksia havaitaan eikä niitä korjata, sertifiointi peruutetaan.”;

30) korvataan 31 artiklan 3 kohta seuraavasti:

”3. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukauden kuluttua tämän muutosasetuksen voimaantulopäivästä] tämän artiklan 1 kohdan vaatimuksiin liittyvät muutoseikat ja menettelyt antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

31) muutetaan 32 artikla seuraavasti:

a) lisätään 1 kohtaan alakohta seuraavasti:

”Jos hyväksytyjen sähköisten allekirjoitusten validointi noudattaa 3 kohdassa tarkoitettuja standardeja, eritelmiä ja menettelyjä, sen katsotaan olevan tämän kohdan ensimmäisessä alakohdassa säädettyjen vaatimusten mukainen.”;

b) korvataan 3 kohta seuraavasti:

”3. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa hyväksytyjen sähköisten allekirjoitusten validointiin sovellettavat eritelmät ja menettelyt antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

32) lisätään artikla seuraavasti:

”32 a artikla

Hyväksytyihin varmenteisiin perustuvien kehittyneiden sähköisten allekirjoitusten validointia koskevat vaatimukset

1. Hyväksytyyn varmenteeseen perustuvan kehittyneen sähköisen allekirjoituksen validointiprosessilla vahvistetaan hyväksytyyn varmenteeseen perustuvan kehittyneen sähköisen allekirjoituksen pätevyys, edellyttäen että:
 - a) allekirjoitusta tukeva varmenne oli allekirjoitushetkellä liitteen I mukainen hyväksytty sähköisen allekirjoituksen varmenne;
 - b) hyväksytyyn varmenteeseen on myöntänyt hyväksytty luottamuspalvelun tarjoaja ja se oli voimassa allekirjoitushetkellä;
 - c) allekirjoituksen validointitiedot vastaavat luottavalle osapuolelle annettuja tietoja;

- d) varmenteen allekirjoittajaa edustava yksilöivä tietokokonaisuus on annettu oikein luottavalle osapuolelle;
 - e) jos allekirjoitushetkellä on käytetty pseudonyymiä, sen käytöstä on selkeästi ilmoitettu luottavalle osapuolelle;
 - f) allekirjoitettujen tietojen eheyttä ei ole loukattu;
 - g) 26 artiklassa säädetyt vaatimukset täyttyivät allekirjoitushetkellä.
2. Hyväksytyyn varmenteeseen perustuvan kehittyneen sähköisen allekirjoituksen validointiin käytettävän järjestelmän on annettava luottavalle osapuolelle validointiprosessissa oikea tulos, ja sen on annettava luottavalle osapuolelle mahdollisuus huomata mahdolliset tietoturvaan vaikuttavat poikkeamat.
3. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa hyväksytyihin varmenteisiin perustuvien kehittyneiden sähköisten allekirjoitusten validointiin sovellettavat eritelvät ja menettelyt antamalla täytäntöönpanosäädöksiä. Jos hyväksytyihin varmenteisiin perustuvien kehittyneiden sähköisten allekirjoitusten validointi vastaa kyseisiä standardeja, erittelyjä ja menettelyjä, sen katsotaan olevan 1 kohdassa säädettyjen vaatimusten mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

33) korvataan 33 artiklan 2 kohta seuraavasti:

”2. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa tämän artiklan 1 kohdassa tarkoitettua hyväksyttyä validointipalvelua koskevat eritelmät ja menettelyt antamalla täytäntöönpanosäädöksiä. Jos hyväksytyjen sähköisten allekirjoitusten hyväksytty validointipalvelu vastaa kyseisiä standardeja, erittelyjä ja menettelyjä, sen katsotaan olevan 1 kohdassa säädettyjen vaatimusten mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

34) muutetaan 34 artikla seuraavasti:

a) lisätään kohta seuraavasti:

”1 a. Jos hyväksytyjen sähköisten allekirjoitusten hyväksyttyä säilyttämispalvelua koskevat järjestelyt vastaavat 2 kohdassa tarkoitettuja standardeja, eritelmiä ja menettelyjä, niiden katsotaan olevan 1 kohdassa säädettyjen vaatimusten mukaisia.”;

b) korvataan 2 kohta seuraavasti:

”2. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa hyväksytyjen sähköisten allekirjoitusten hyväksytyihin säilyttämispalveluihin sovellettavat eritelmät ja menettelyt antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

35) kumotaan 35 artiklan 3 kohta;

36) muutetaan 36 artikla seuraavasti:

a) ainoasta kohdasta tulee 1 kohta;

b) lisätään kohta seuraavasti:

”2. Komissio arvioi viimeistään ... päivänä ...kuuta ... [24 kuukauden kuluttua tämän muutosasetuksen voimaantulopäivästä], onko tarpeen antaa täytäntöönpanosäädöksiä, joissa vahvistetaan luettelo viitestandardeista ja tarvittaessa kehittyneitä sähköisiä leimoja koskevat eritelmät ja menettelyt. Komissio voi kyseisen arvioinnin perusteella antaa tällaisia täytäntöönpanosäädöksiä. Kehittyneitä sähköisiä leimoja koskevien vaatimusten katsotaan täyttyvän, kun kehittynyt sähköinen leima on kyseisten standardien, eritelmien ja menettelyjen mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

37) kumotaan 37 artiklan 4 kohta;

38) korvataan 38 artiklan 6 kohta seuraavasti:

”6. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa eritelmät ja menettelyt sähköisen leiman hyväksytyjä varmenteita varten antamalla täytäntöönpanosäädöksiä. Jos sähköisen leiman hyväksyty varmenne vastaa kyseisiä standardeja, eritelmiä ja menettelyjä, sen katsotaan olevan liitteessä III säädettyjen vaatimusten mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

39) lisätään artikla seuraavasti:

”39 a artikla

Hyväksytyjen sähköisen leiman etäluontivälineiden hallinnoinnin hyväksytyä palvelua koskevat vaatimukset

Hyväksytyjen sähköisen leiman etäluontivälineiden hallinnointiin hyväksytyyn palveluun sovelletaan soveltuvin osin 29 a artiklaa.”;

40) lisätään III luvun 5 jaksoon artikla seuraavasti:

”40 a artikla

Hyväksytyihin varmenteisiin perustuvien kehittyneiden sähköisten leimojen validointia koskevat vaatimukset

Edellä olevaa 32 a artiklaa sovelletaan soveltuvin osin hyväksytyihin varmenteisiin perustuvien kehittyneiden sähköisten leimojen validointiin.”;

41) kumotaan 41 artiklan 3 kohta;

42) muutetaan 42 artikla seuraavasti:

a) lisätään kohta seuraavasti:

”1 a. Jos päivän ja ajankohdan sitominen tietoihin ja aikälähteen virheettömyys vastaavat 2 kohdassa tarkoitettuja standardeja, eritelmiä ja menettelyitä, niiden katsotaan olevan 1 kohdassa säädettyjen vaatimusten mukaiset.”;

b) korvataan 2 kohta seuraavasti:

”2. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa eritelmit ja menettelyt päivän ja ajankohdan sitomista tietoihin ja aikälähteen virheettömyyttä varten antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

43) muutetaan 44 artikla seuraavasti:

a) lisätään kohta seuraavasti:

”1 a. Jos tietojen lähettämisen- ja vastaanottamisprosessi vastaa 2 kohdassa tarkoitettuja standardeja, eritelmiä ja menettelyitä, sen katsotaan olevan 1 kohdassa säädettyjen vaatimusten mukainen.”;

b) korvataan 2 kohta seuraavasti:

”2. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa eritelmät ja menettelyt tietojen lähettämisen- ja vastaanottamisprosessia varten antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

c) lisätään kohdat seuraavasti:

”2 a. Hyväksytyjen sähköisten rekisteröityjen jakelupalvelujen tarjoajat voivat sopia tarjoamiensa hyväksytyjen sähköisten rekisteröityjen jakelupalvelujen välisestä yhteentoimivuudesta. Tällaisen yhteentoimivuuskehysten on oltava 1 kohdassa säädettyjen vaatimusten mukainen, ja vaatimustenmukaisuuden arviointilaitoksen on vahvistettava tällainen vaatimustenmukaisuus.

2 b. Komissio voi vahvistaa luettelon viitestandardeista ja tarvittaessa eritelmät ja menettelyt tämän artiklan 2 a kohdassa tarkoitettua yhteentoimivuuskehystä varten antamalla täytäntöönpanosäädöksiä. Teknisten eritelmien ja standardien sisällön on oltava kustannustehokkaita ja oikeasuhteisia. Täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

44) korvataan 45 artikla seuraavasti:

”45 artikla

Verkkosivustojen todentamisen hyväksytyjä varmenteita koskevat vaatimukset

1. Verkkosivustojen todentamisen hyväksytyjen varmenteiden on täytettävä liitteessä IV säädetty vaatimukset. Kyseisten vaatimusten noudattamista on arvioitava tämän artiklan 2 kohdassa tarkoitettujen standardien, eritelmien ja menettelyjen mukaisesti.
 - 1 a. Verkkoselainten tarjoajien on tunnustettava tämän artiklan 1 kohdan mukaisesti myönnetty verkkosivustojen todentamisen hyväksytyt varmenteet. Verkkoselainten tarjoajien on varmistettava, että varmenteessa todistetut henkilöllisyystiedot ja muut todistetut attribuutit esitetään käyttäjäystävällisellä tavalla. Verkkoselainten tarjoajien on varmistettava tuki tämän artiklan 1 kohdassa tarkoitetuille verkkosivustojen todentamisen hyväksytyille varmenteille ja yhteentoimivuus niiden kanssa, lukuun ottamatta mikroyrityksiä ja pieniä yrityksiä, sellaisina kuin ne ovat määriteltyinä suosituksen 2003/361/EY liitteessä olevassa 2 artiklassa, niiden viiden ensimmäisen vuoden aikana, joina ne toimivat verkkoselainpalvelujen tarjoajina.
 - 1 b. Verkkosivustojen todentamisen hyväksytyille varmenteille ei saa asettaa muita pakollisia vaatimuksia kuin ne, joista säädetään 1 kohdassa.

2. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa eritelmät ja menettelyt tämän artiklan 1 kohdassa tarkoitettuja verkkosivustojen todentamisen hyväksytyjä varmenteita varten antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

45) lisätään artikla seuraavasti:

”45 a artikla

Kyberturvallisuutta koskevat varotoimenpiteet

1. Verkkoselainten tarjoajat eivät saa toteuttaa minkäänlaisia toimenpiteitä, jotka ovat vastoin niille 45 artiklassa asetettuja velvoitteita, erityisesti vaatimuksia tunnustaa verkkosivustojen todentamisen hyväksytyt varmenteet ja esittää annetut henkilöllisyystiedot käyttäjäystävällisellä tavalla.
2. Poiketen siitä, mitä 1 kohdassa säädetään, ja ainoastaan sellaisten perusteltujen huolenaiheiden tapauksessa, jotka koskevat tietoturvaloukkauksia tai yksilöidyn varmenteen tai varmennejoukon eheyden menetystä, verkkoselainten tarjoajat voivat toteuttaa varotoimenpiteitä kyseisen varmenteen tai varmennesarjan suhteen.

3. Kun verkkoselainten tarjoaja toteuttaa varotoimenpiteitä 2 kohdan nojalla, verkkoselainten tarjoajan on ilmoitettava huolenaiheensa kirjallisesti ilman aiheetonta viivytystä, mukaan lukien kuvaus toimenpiteistä kyseisten huolenaiheiden lieventämiseksi, komissiolle, toimivaltaiselle valvontaelimelle, taholle, jolle varmenne on myönnetty, ja kyseisen varmenteen tai varmennesarjan myöntäneelle hyväksytylle luottamuspalvelun tarjoajalle. Saatuaan tällaisen ilmoituksen toimivaltaisen valvontaelimen on annettava kyseisen verkkoselaimen tarjoajalle vastaanottoilmoitus.

4. Toimivaltaisen valvontaelimen on tutkittava seikkoja, jotka on esitetty 46 b artiklan 4 kohdan k alakohdan mukaisessa ilmoituksessa. Jos kyseisen selvityksen tulos ei johda varmenteen hyväksytyin aseman peruuttamiseen, valvontaelimen on ilmoitettava asiasta verkkoselaimen tarjoajalle ja pyydetävä kyseistä tarjoajaa lopettamaan tämän artiklan 2 kohdassa tarkoitetut varotoimenpiteet.”;

46) lisätään III lukuun jaksot seuraavasti:

”9 JAKSO

SÄHKÖINEN ATTRIBUUTTITODISTUS

45 b artikla

Sähköisen attribuuttitodistuksen oikeusvaikutukset

1. Sähköisen attribuuttitodistuksen oikeusvaikutuksia tai käytettävyyttä todisteena oikeudellisissa menettelyissä ei voida kieltää pelkästään sen takia, että se on sähköisessä muodossa tai että se ei täytä hyväksytyjen sähköisten attribuuttitodistusten vaatimuksia.
2. Hyväksytyllä sähköisellä attribuuttitodistuksella ja virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämällä tai sen puolesta myönnettyillä attribuuttitodistuksilla on sama oikeusvaikutus kuin laillisesti paperimuodossa myönnettyillä todistuksilla.
3. Virallisesta lähteestä yhdessä jäsenvaltiossa vastaavan julkisen sektorin elimen myöntämä tai sen puolesta myönnetty attribuuttitodistus on tunnustettava kaikissa jäsenvaltioissa virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämäksi tai sen puolesta myönnettyksi attribuuttitodistukseksi.

45 c artikla

Sähköisen attribuuttitodistuksen käyttö julkisissa palveluissa

Kun julkisen sektorin elimen tarjoaman verkkopalvelun käyttö edellyttää kansallisen oikeuden nojalla sähköistä tunnistamista sähköisen tunnistamisen menetelmän ja todentamisen avulla, sähköiseen attribuuttitodistukseen sisältyvät henkilön tunnistetiedot eivät saa korvata sähköisen tunnistamisen menetelmän ja todentamisen avulla tehtävää sähköistä tunnistamista, ellei jäsenvaltio sitä nimenomaisesti salli. Tällöin on hyväksyttävä myös muissa jäsenvaltioissa myönnettyt hyväksytyt sähköiset attribuuttitodistukset.

45 d artikla

Hyväksytyt sähköisiä attribuuttitodistuksia koskevat vaatimukset

1. Hyväksytyjen sähköisten attribuuttitodistusten on täytettävä liitteessä V säädetyt vaatimukset.
2. Liitteessä V säädettyjen vaatimusten noudattamista arvioidaan tämän artiklan 5 kohdassa tarkoitettujen standardien, eritelmien ja menettelyjen mukaisesti.
3. Hyväksytyille sähköisille attribuuttitodistuksille ei saa asettaa muita pakollisia vaatimuksia liitteessä V säädettyjen vaatimusten lisäksi.
4. Jos hyväksytty sähköinen attribuuttitodistus on peruttu sen ensimmäisen myöntämisen jälkeen, sen voimassaolo päättyy peruuttamisajankohdasta lähtien, eikä sen tilaa voida missään olosuhteissa palauttaa.

5. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [kuusi kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa eritelmät ja menettelyt hyväksytyjä sähköisiä attribuuttitodistuksia varten antamalla täytäntöönpanosäädöksiä. Kyseisten täytäntöönpanosäädösten on oltava johdonmukaisia eurooppalaisen digitaalisen identiteetin lompakon toteuttamista koskevassa 5 a artiklan 23 kohdassa tarkoitettujen täytäntöönpanosäädösten kanssa. Ne hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

45 e artikla

Attribuuttien tarkastaminen virallisista lähteistä

1. Jäsenvaltioiden on varmistettava 24 kuukauden kuluessa 5 a artiklan 23 kohdassa ja 5 c artiklan 6 kohdassa tarkoitettujen täytäntöönpanosäädösten voimaantulopäivästä, että ainakin liitteessä VI lueteltujen attribuuttien osalta toteutetaan toimenpiteitä, joiden avulla sähköisten attribuuttitodistusten hyväksytyt luottamuspalvelun tarjoajat voivat tarkastaa kyseiset attribuutit sähköisesti käyttäjän pyynnöstä unionin oikeuden tai kansallisen lainsäädännön mukaisesti, jos kyseiset attribuutit perustuvat julkisen sektorin virallisiin lähteisiin.
2. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [kuusi kuukautta tämän muutosasetuksen voimaantulopäivästä] täytäntöönpanosäädöksillä luettelon viitestandardeista ja tarvittaessa eritelmät ja menettelyt attribuuttien luetteloa varten sekä attribuuttitodistusten myöntämisen järjestelmät ja hyväksytyjen sähköisten attribuuttitodistusten tarkastamisen menettelyt tämän artiklan 1 kohdan soveltamiseksi ottaen huomioon asiaa koskevat kansainväliset standardit. Kyseisten täytäntöönpanosäädösten on oltava johdonmukaisia eurooppalaisen digitaalisen identiteetin lompakon toteuttamista koskevassa 5 a artiklan 23 kohdassa tarkoitettujen täytäntöönpanosäädösten kanssa. Ne hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

45 f artikla

Virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämää tai sen puolesta myönnettyä sähköistä attribuuttitodistusta koskevat vaatimukset

1. Virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämän tai sen puolesta myönnetyn sähköisen attribuuttitodistuksen on täytettävä seuraavat vaatimukset:
 - a) liitteessä VII vahvistetut vaatimukset;
 - b) hyväksytyt varmenne, joka tukee liitteessä VII olevassa b alakohdassa tarkoitettuksi myöntäjäksi nimetyn, 3 artiklan 46 alakohdassa tarkoitetun julkisen sektorin elimen hyväksytyä sähköistä allekirjoitusta tai hyväksytyä sähköistä leimaa ja joka sisältää tietyt automaattiseen käsittelyyn soveltuvassa muodossa olevat varmennetut attribuutit ja jossa:
 - i) ilmoitetaan, että todistuksen myöntävä elin on perustettu unionin oikeuden tai kansallisen lainsäädännön mukaisesti elimeksi, joka on vastuussa siitä virallisesta lähteestä, jonka perusteella sähköinen attribuuttitodistus myönnetään, tai elimeksi, joka on nimetty toimimaan edellisen puolesta;
 - ii) annetaan tietoja, jotka yksiselitteisesti edustavat i alakohdassa tarkoitettua virallista lähdettä; ja
 - iii) määritellään i alakohdassa tarkoitettu unionin oikeus tai kansallinen lainsäädäntö.

2. Jäsenvaltion, johon 3 artiklan 46 alakohdassa tarkoitettujen julkisen sektorin elimien sijaintipaikat, on varmistettava, että sähköisiä attribuuttitodistuksia myöntävät julkisen sektorin elimet ovat yhtä luotettavia kuin 24 artiklan mukaisesti hyväksytyt luottamuspalvelun tarjoajat.
3. Jäsenvaltioiden on ilmoitettava komissiolle 3 artiklan 46 alakohdassa tarkoitettujen julkisen sektorin elimien. Ilmoitukseen on sisällyttävä vaatimustenmukaisuuden arviointilaitoksen laatima vaatimustenmukaisuuden arviointiraportti, jossa vahvistetaan, että tämän artiklan 1, 2 ja 6 kohdassa säädetyt vaatimukset täyttyvät. Komissio asettaa yleisön saataville suojatusti luettelon 3 artiklan 46 alakohdassa tarkoitetuista julkisen sektorin elimistä sähköisesti allekirjoitetussa tai leimatussa muodossa, joka soveltuu automaattiseen käsittelyyn.
4. Jos virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämä tai sen puolesta myönnetty sähköinen attribuuttitodistus peruutetaan todistuksen ensimmäisen myöntämisen jälkeen, sen voimassaolo päättyy sen peruuttamisajankohdasta lähtien ja sen tilaa ei palauteta.
5. Virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämän tai sen puolesta myönnetyn sähköisen attribuuttitodistuksen katsotaan olevan 1 kohdassa säädettyjen vaatimusten mukainen, jos se täyttää 6 kohdassa tarkoitettujen standardien, eritelmien ja menettelyt.

6. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [kuusi kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa eritelmät ja menettelyt virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämää tai sen puolesta myönnettyä sähköistä attribuuttitodistusta varten antamalla täytäntöönpanosäädöksiä. Kyseisten täytäntöönpanosäädösten on oltava johdonmukaisia eurooppalaisen digitaalisen identiteetin lompakon toteuttamista koskevassa 5 a artiklan 23 kohdassa tarkoitettujen täytäntöönpanosäädösten kanssa. Ne hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.
7. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [kuusi kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa eritelmät ja menettelyt tämän artiklan 3 kohdan soveltamista varten antamalla täytäntöönpanosäädöksiä. Kyseisten täytäntöönpanosäädösten on oltava johdonmukaisia eurooppalaisen digitaalisen identiteetin lompakon toteuttamista koskevassa 5 a artiklan 23 kohdassa tarkoitettujen täytäntöönpanosäädösten kanssa. Ne hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.
8. Sähköisten attribuuttitodistusten 3 artiklan 46 alakohdassa tarkoitettujen myöntäjien on tarjottava rajapinta 5 a artiklan mukaisesti tarjottuihin eurooppalaisiin digitaalisen identiteetin lompakoihin.

45 g artikla

Sähköisten attribuuttitodistusten myöntäminen eurooppalaisiin digitaalisen identiteetin lompakoihin

1. Sähköisten attribuuttitodistusten tarjoajien on annettava eurooppalaisen digitaalisen identiteetin lompakon käyttäjille mahdollisuus pyytää, saada, tallentaa ja hallinnoida sähköisiä attribuuttitodistuksia riippumatta siitä, missä jäsenvaltiossa eurooppalainen digitaalisen identiteetin lompakko tarjotaan.
2. Hyväksytyjen sähköisten attribuuttitodistusten tarjoajien on tarjottava rajapinta 5 a artiklan mukaisesti tarjottuihin eurooppalaisiin digitaalisen identiteetin lompakoihin.

45 h artikla

Sähköisiin attribuuttitodistuksiin liittyvien palvelujen tarjoamista koskevat lisäsäännöt

1. Hyväksytyihin ja ei-hyväksytyihin sähköisiin attribuuttitodistuksiin liittyvien palvelujen tarjoajat eivät saa yhdistää kyseisten palvelujen tarjoamiseen liittyviä henkilötietoja sellaisiin henkilötietoihin, jotka ovat peräisin muista kyseisten palvelujen tarjoajien tai niiden liikekumppaneiden tarjoamista palveluista.
2. Sähköisiin attribuuttitodistuksiin liittyvien palvelujen tarjoamiseen liittyvät henkilötiedot on pidettävä loogisesti erillään muista sähköisten attribuuttitodistusten tarjoajan hallussa olevista tiedoista.
3. Hyväksytyihin sähköisiin attribuuttitodistuksiin liittyvien palvelujen tarjoajien on toteutettava tällaisten hyväksytyjen luottamuspalvelujen tarjoaminen tavalla, joka on toiminnallisesti erillään muista niiden tarjoamista palveluista.

10 JAKSO

SÄHKÖISET ARKISTOINTIPALVELUT

45 i artikla

Sähköisten arkistointipalvelujen oikeusvaikutukset

1. Sähköistä arkistointipalvelua käyttäen säilytettyjen sähköisten tietojen ja sähköisten asiakirjojen oikeusvaikutuksia tai käytettävyyttä todisteena oikeudellisissa menettelyissä ei voida kieltää pelkästään sillä perusteella, että ne ovat sähköisessä muodossa tai että niitä ei ole säilytetty käyttäen hyväksyttyä sähköistä arkistointipalvelua.
2. Hyväksyttyä sähköistä arkistointipalvelua käyttäen säilytettyihin sähköisiin tietoihin ja sähköisiin asiakirjoihin sovelletaan olettaa niiden eheydestä ja alkuperästä kokonaisuutena, jonka ne ovat hyväksytyt luottamuspalvelun tarjoajan säilytettävänä.

45 j artikla

Hyväksytyt sähköisiä arkistointipalveluja koskevat vaatimukset

1. Hyväksytyt sähköisten arkistointipalvelujen on täytettävä seuraavat vaatimukset:
 - a) niitä tarjoavat hyväksytyt luottamuspalvelun tarjoajat;
 - b) ne käyttävät menettelyjä ja teknologioita, joilla voidaan varmistaa sähköisten tietojen ja sähköisten asiakirjojen pysyvyys ja luettavuus teknologista voimassaoloaika pidemmälle ja ainakin koko lakisääteisen tai sopimusperusteisen säilytysajan ja säilyttää samalla tietojen eheys ja niiden alkuperän virheettömyys;

- c) ne varmistavat, että kyseiset sähköiset tiedot ja kyseiset sähköiset asiakirjat säilytetään siten, että ne suojataan häviämislähteen ja muuttumiselta, lukuun ottamatta niiden tallennusvälinettä tai sähköistä muotoa koskevia muutoksia;
- d) ne antavat valtuutetuille luottaville osapuolille mahdollisuuden saada automaattisesti ilmoitus, jolla vahvistetaan, että hyväksytyistä sähköisistä arkistosta haettaviin sähköisiin tietoihin ja sähköisiin asiakirjoihin sovelletaan oletettavaa tietojen eheydestä säilyttämisaikojen alusta hakuhetkeen asti.

Ensimmäisen alakohdan d alakohdassa tarkoitettu ilmoitus toimitetaan luotettavalla ja tehokkaalla tavalla, ja siinä on hyväksytyin sähköisen arkistointipalvelun tarjoajan hyväksyty sähköinen allekirjoitus tai hyväksyty sähköinen leima.

2. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] luettelon viitestandardeista ja tarvittaessa eritelmät ja menettelyt hyväksytyjä sähköisiä arkistointipalveluja varten antamalla täytäntöönpanosäädöksiä. Hyväksytyjä sähköisiä arkistointipalveluja koskevien vaatimusten katsotaan täyttyvän, kun hyväksyty sähköinen arkistointipalvelu täyttää kyseiset standardit, eritelmät ja menettelyt. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

11 JAKSO

SÄHKÖISET TILIKIRJAT

45 k artikla

Sähköisten tilikirjojen oikeusvaikutukset

1. Sähköisen tilikirjan oikeusvaikutuksia tai käytettävyyttä todisteena oikeudellisissa menettelyissä ei voida kieltää pelkästään sillä perusteella, että se on sähköisessä muodossa tai että se ei täytä hyväksytyjen sähköisten tilikirjojen vaatimuksia.
2. Hyväksytyyn sähköisen tilikirjan tietueisiin liitetään oletta, jonka mukaan ne ovat yksilöllisessä ja oikeellisessa peräkkäisessä kronologisessa järjestyksessä ja eheitä.

45 l artikla

Hyväksytyjä sähköisiä tilikirjoja koskevat vaatimukset

1. Hyväksytyjen sähköisten tilikirjojen on täytettävä seuraavat vaatimukset:
 - a) ne luo ja niitä hallinnoi yksi tai useampi hyväksytty luottamuspalvelun tarjoaja;
 - b) ne vahvistavat tilikirjassa olevien tietueiden alkuperän;
 - c) ne varmistavat tilikirjan tietueiden yksilöllisen peräkkäisen kronologisen järjestyksen;
 - d) ne tallentavat tiedot siten, että tietojen mahdollinen myöhempi muuttaminen voidaan havaita välittömästi, mikä varmistaa tietojen eheyden pitkällä aikavälillä.

2. Jos sähköinen tilikirja vastaa 3 kohdassa tarkoitettuja standardeja, eritelmiä ja menettelyjä, sen katsotaan olevan 1 kohdassa säädettyjen vaatimusten mukainen.
3. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] täytäntöönpanosäädöksin luettelon viitestandardeista ja tarvittaessa tämän artiklan 1 kohdassa säädettyjä vaatimuksia koskevat eritelmit ja menettelyt. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

47) lisätään luku seuraavasti:

”IV a LUKU

HALLINTOKEHYS

46 a artikla

Eurooppalaisen digitaalisen identiteetin lompakon kehysten valvonta

1. Jäsenvaltioiden on nimettävä valvontaelin tai valvontaelimiä, jotka ovat sijoittautuneet niiden alueelle.

Ensimmäisen alakohdan mukaisesti nimetyille valvontaelimille on annettava tarvittavat valtuudet ja riittävät resurssit suorittaa tehtävänsä tuloksellisesti, tehokkaasti ja riippumattomasti.

2. Jäsenvaltioiden on ilmoitettava komissiolle 1 kohdan mukaisesti nimettyjen valvontaelimien nimet ja osoitteet ja niiden mahdolliset myöhemmät muutokset. Komissio julkaisee luettelon ilmoitetuista valvontaelimistä.
3. Edellä olevan 1 kohdan mukaisesti nimettyjen valvontaelinten rooli on seuraava:
 - a) nimeävän jäsenvaltion alueelle sijoittautuneiden eurooppalaisten digitaalisen identiteetin lompakkojen tarjoajien valvonta ja sen varmistaminen ennakkoon ja jälkikäteen toteutettavin valvontatoimin, että nämä tarjoajat ja niiden tarjoamat eurooppalaiset digitaalisen identiteetin lompakot täyttävät tässä asetuksessa säädetyt vaatimukset;
 - b) toimien toteuttaminen tarvittaessa nimeävän jäsenvaltion alueelle sijoittautuneiden eurooppalaisten digitaalisen identiteetin lompakkojen tarjoajien suhteen jälkikäteen toteutettavin valvontatoimin, jos sille ilmoitetaan, että tarjoajat tai niiden tarjoamat eurooppalaiset digitaalisen identiteetin lompakot rikkovat tätä asetusta.
4. Edellä olevan 1 kohdan mukaisesti nimettyjen valvontaelinten tehtäviin kuuluvat erityisesti seuraavat:
 - a) yhteistyön tekeminen muiden valvontaelinten kanssa ja tuen antaminen niille 46 c ja 46 e artiklan mukaisesti;
 - b) tämän asetuksen noudattamisen seuraamiseksi tarvittavien tietojen pyytäminen;

- c) ilmoittaminen direktiivin (EU) 2022/2555 8 artiklan 1 kohdan mukaisesti nimetyille tai perustetuille asianomaisten jäsenvaltioiden asiaankuuluville toimivaltaisille viranomaisille kaikista merkittävistä tietoturvaloukkauksista tai eheyden menetyksistä, joista ne saavat tiedon tehtäviään suorittaessaan, ja jos merkittävä tietoturvaloukkaus tai eheyden menetys koskee muita jäsenvaltioita, ilmoittaminen asiasta direktiivin (EU) 2022/2555 8 artiklan 3 kohdan mukaisesti nimetyille tai perustetulle asianomaisen jäsenvaltion keskitetylle yhteyspisteelle ja tämän asetuksen 46 c artiklan 1 kohdan mukaisesti nimetyille keskitetyille yhteyspisteille asianomaisissa muissa jäsenvaltioissa sekä tiedottaminen asiasta yleisölle tai sen vaatiminen, että eurooppalaisen digitaalisen identiteetin lompakon tarjoaja tiedottaa siitä, jos valvontaelin katsoo, että tietoturvaloukkauksen tai eheyden menetyksen julkistaminen olisi yleisen edun mukaista;
- d) paikalla tehtävien tarkastusten ja muun kuin paikalla toteutettavan valvonnan suorittaminen;
- e) sen edellyttäminen, että eurooppalaisen digitaalisen identiteetin lompakon tarjoajat korjaavat mahdolliset puutteet tässä asetuksessa säädettyjen vaatimusten täyttämiseksi;
- f) luottavien osapuolten rekisteröinnin tai 5 b artiklan 7 kohdassa tarkoitettuun yhteiseen mekanismiin sisällyttämisen keskeyttäminen tai peruuttaminen, jos eurooppalaista digitaalisen identiteetin lompakkoa käytetään laittomasti tai vilpillisesti;
- g) yhteistyön tekeminen asetuksen (EU) 2016/679 51 artiklan nojalla perustettujen toimivaltaisten valvontaviranomaisten kanssa erityisesti ilmoittamalla niille ilman aiheutonta viivytystä, jos henkilötietojen suoja koskevia sääntöjä näyttää olevan rikottu, sekä tietoturvaloukkauksista, jotka näyttävät olevan henkilötietojen loukkauksia.

5. Jos 1 kohdan mukaisesti nimetty valvontaelin vaatii eurooppalaisen digitaalisen identiteetin lompakon tarjoajaa 4 kohdan e alakohdan nojalla korjaamaan mahdollisen laiminlyönnin tämän asetuksen mukaisten vaatimusten noudattamisessa ja kyseinen tarjoaja ei toimi pyynnön mukaisesti ja valvontaelimen tapauksen mukaan asettaman aikarajan puitteissa, 1 kohdan mukaisesti nimetty valvontaelin voi erityisesti laiminlyönnin laajuuden, keston ja seuraukset huomioon ottaen määrätä tarjoajan keskeyttämään tai lopettamaan eurooppalaisen digitaalisen identiteetin lompakon tarjoamisen. Valvontaelimen on ilman aiheetonta viivytystä ilmoitettava muiden jäsenvaltioiden valvontaelimille, komissiolle, luottaville osapuolille ja Euroopan digitaalisen identiteetin lompakon käyttäjille päätöksestä vaatia eurooppalaisen digitaalisen identiteetin lompakon tarjoamisen keskeyttämistä tai lopettamista.
6. Kunkin 1 kohdan mukaisesti nimetyn valvontaelimen on toimitettava komissiolle joka vuosi viimeistään 31 päivänä maaliskuuta kertomus tärkeimmistä toimistaan edellisenä kalenterivuonna. Komissio asettaa kyseiset vuosikertomukset Euroopan parlamentin ja neuvoston saataville.
7. Komissio vahvistaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] tämän artiklan 6 kohdassa tarkoitettuun kertomukseen liittyvät muutoseikat ja menettelyt antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

46 b artikla

Luottamuspalvelujen valvonta

1. Jäsenvaltioiden on nimettävä niiden alueelle sijoittautunut valvontaelin tai nimettävä keskinäisellä sopimuksella toisen jäsenvaltion kanssa valvontaelin, joka on sijoittautunut kyseiseen toiseen jäsenvaltioon. Kyseinen valvontaelin vastaa valvontatehtävistä nimeävässä jäsenvaltiossa luottamuspalvelun tarjoamisen osalta.

Ensimmäisen alakohdan mukaisesti nimetyille valvontaelimille on annettava tarvittavat valtuudet ja riittävät resurssit suorittaa tehtävänsä.

2. Jäsenvaltioiden on ilmoitettava komissiolle 1 kohdan mukaisesti nimettyjen valvontaelimien nimet ja osoitteet ja niiden mahdolliset myöhemmät muutokset. Komissio julkaisee luettelon ilmoitetuista valvontaelimistä.

3. Edellä olevan 1 kohdan mukaisesti nimettyjen valvontaelinten rooli on seuraava:

- a) nimeävän jäsenvaltion alueelle sijoittautuneiden hyväksytyjen luottamuspalvelun tarjoajien valvonta ja sen varmistaminen ennakkoon ja jälkikäteen toteutettavin valvontatoimin, että nämä hyväksytyt luottamuspalvelun tarjoajat ja niiden tarjoamat hyväksytyt luottamuspalvelut täyttävät tässä asetuksessa säädetyt vaatimukset;
- b) toimien toteuttaminen tarvittaessa nimeävän jäsenvaltion alueelle sijoittautuneiden ei-hyväksytyjen luottamuspalvelun tarjoajien suhteen jälkikäteen toteutettavin valvontatoimin, jos sille ilmoitetaan, että nämä ei-hyväksytyt luottamuspalvelun tarjoajat tai niiden tarjoamat luottamuspalvelut eivät väitetysti täytä tässä asetuksessa säädettyjä vaatimuksia.

4. Tämän artiklan 1 kohdan mukaisesti nimetyn valvontaelimen tehtäviin kuuluvat erityisesti seuraavat:
- a) ilmoittaminen direktiivin (EU) 2022/2555 8 artiklan 1 kohdan mukaisesti nimetyille tai perustetuille asianomaisten jäsenvaltioiden asiaankuuluville toimivaltaisille viranomaisille kaikista merkittävistä tietoturvaloukkauksista tai eheyden menetyksistä, joista se saa tiedon tehtäviään suorittaessaan, ja jos merkittävä tietoturvaloukkaus tai eheyden menetys koskee muita jäsenvaltioita, ilmoittaminen asiasta direktiivin (EU) 2022/2555 8 artiklan 3 kohdan mukaisesti nimetyille tai perustetulle asianomaisen jäsenvaltion keskitetylle yhteyspisteelle ja tämän asetuksen 46 c artiklan 1 kohdan mukaisesti nimetyille keskitetyille yhteyspisteille asianomaisissa muissa jäsenvaltioissa sekä tiedottaminen asiasta yleisölle tai sen vaatiminen, että luottamuspalvelun tarjoaja tiedottaa siitä, jos valvontaelin katsoo, että tietoturvaloukkauksen tai eheyden menetyksen julkistaminen olisi yleisen edun mukaista;
 - b) yhteistyön tekeminen muiden valvontaelinten kanssa ja tuen antaminen niille 46 c ja 46 e artiklan mukaisesti;
 - c) 20 artiklan 1 kohdassa ja 21 artiklan 1 kohdassa tarkoitettujen vaatimustenmukaisuuden arviointikertomusten analysointi;
 - d) komissiolle tiedottaminen valvontaelimen tärkeimmistä toimista tämän artiklan 6 kohdan mukaisesti;

- e) tarkastusten tekeminen tai vaatimustenmukaisuuden arviointilaitoksen pyytäminen suorittamaan hyväksytyjen luottamuspalvelun tarjoajien vaatimustenmukaisuuden arviointi 20 artiklan 2 kohdan mukaisesti;
- f) yhteistyön tekeminen asetuksen (EU) 2016/679 51 artiklan nojalla perustettujen toimivaltaisten valvontaviranomaisten kanssa erityisesti ilmoittamalla niille ilman aiheetonta viivytystä, jos henkilötietojen suojaa koskevia sääntöjä näyttää olevan rikottu, sekä tietoturvaloukkauksista, jotka näyttävät olevan henkilötietojen loukkauksia;
- g) hyväksytyt aseman myöntäminen luottamuspalvelun tarjoajille ja niiden tarjoamille palveluille sekä kyseisen aseman peruuttaminen 20 ja 21 artiklan mukaisesti;
- h) 22 artiklan 3 kohdassa tarkoitettusta kansallisesta luotetusta luettelosta vastaavalle elimelle tiedottaminen hyväksytyt aseman myöntämisestä tai peruuttamisesta koskevista päätöksistään, ellei tämä elin ole myös tämän artiklan 1 kohdan mukaisesti nimetty valvontaelin;
- i) lopettamissuunnitelmia koskevien säännösten olemassaolon ja asianmukaisen soveltamisen tarkistaminen, jos hyväksytty luottamuspalvelun tarjoaja lopettaa toimintansa, 24 artiklan 2 kohdan h alakohdan mukainen tiedon saatavilla pitäminen mukaan lukien;
- j) sen edellyttäminen, että luottamuspalvelun tarjoajat korjaavat mahdolliset puutteet tässä asetuksessa säädettyjen vaatimusten täyttämiseksi;
- k) verkkoselainten tarjoajien 45 a artiklan nojalla esittämien väitteiden tutkiminen ja toimien toteuttaminen tarvittaessa.

5. Jäsenvaltiot voivat vaatia, että 1 kohdan mukaisesti nimetty valvontaelin perustaa luottamusinfrastruktuurin ja pitää sitä yllä sekä saattaa sen ajan tasalle kansallisen lain mukaisesti.
6. Kunkin 1 kohdan mukaisesti nimetyn valvontaelimen on toimitettava komissiolle joka vuosi viimeistään 31 päivänä maaliskuuta kertomus tärkeimmistä toimistaan edellisenä kalenterivuonna. Komissio asettaa kyseiset vuosikertomukset Euroopan parlamentin ja neuvoston saataville.
7. Komissio hyväksyy viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] ohjeet siitä, miten tämän artiklan 1 kohdan mukaisesti nimetyt valvontaelimet hoitavat tämän artiklan 4 kohdassa tarkoitettuja tehtäviä, ja vahvistaa täytäntöönpanosäädöksin tämän artiklan 6 kohdassa tarkoitettuun kertomukseen liittyvät muutoseikat ja menettelyt. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

46 c artikla

Keskitetty yhteyspisteet

1. Kunkin jäsenvaltion on nimettävä keskitetty yhteyspiste luottamuspalveluja, eurooppalaisia digitaalisen identiteetin lompakkoja ja ilmoitettuja sähköisen tunnistamisen järjestelmiä varten.

2. Kunkin keskitetyn yhteyspisteen tehtävänä on yhteydenpito rajatylittävän yhteistyön helpottamiseksi luottamuspalvelun tarjoajien valvontaelinten ja eurooppalaisen digitaalisen identiteetin lompakkojen tarjoajien valvontaviranomaisten välillä ja tarvittaessa komission ja Euroopan unionin kyberturvallisuusviraston (ENISA) kanssa sekä jäsenvaltionsa muiden toimivaltaisten viranomaisten kanssa.
3. Kunkin jäsenvaltion on julkistettava ja ilmoitettava komissiolle ilman aiheetonta viivytystä 1 kohdan mukaisesti nimettyjen keskitettyjen yhteyspisteiden nimet ja osoitteet ja niiden mahdolliset myöhemmät muutokset.
4. Komissio julkaisee 3 kohdan mukaisesti ilmoitettujen keskitettyjen yhteyspisteiden luettelon.

46 d artikla

Keskinäinen avunanto

1. Tämän asetuksen mukaisten velvoitteiden valvonnan ja täytäntöönpanon helpottamiseksi 46 a artiklan 1 kohdan ja 46 b artiklan 1 kohdan mukaisesti nimetyt valvontaelimet voivat pyytää, mukaan lukien 46 e artiklan 1 kohdan mukaisesti perustetun yhteistyöryhmän kautta, keskinäistä apua sellaisen toisen jäsenvaltion valvontaelimiltä, johon eurooppalaisen digitaalisen identiteetin lompakon tarjoaja tai luottamuspalvelun tarjoaja on sijoittautunut tai jossa sen verkko ja tietojärjestelmät sijaitsevat tai jossa sen palveluja tarjotaan.

2. Keskinäiseen avunantoon on kuuluttava vähintään seuraavaa:
- a) valvonta- tai täytäntöönpanotoimenpiteitä jäsenvaltiossa soveltavan valvontaelimen on informoitava ja kuultava asianomaisen toisen jäsenvaltion valvontaelintä;
 - b) valvontaelin voi pyytää asianomaisen toisen jäsenvaltion valvontaelintä toteuttamaan valvonta- tai täytäntöönpanotoimenpiteitä mukaan lukien esimerkiksi pyynnöt suorittaa 20 ja 21 artiklassa tarkoitettuihin luottamuspalvelujen tarjoamista koskeviin vaatimustenmukaisuuden arviointikertomuksiin liittyviä selvityksiä;
 - c) valvontaelimet voivat tarvittaessa toteuttaa yhteisselvityksiä muiden jäsenvaltioiden valvontaelinten kanssa.

Asianomaiset jäsenvaltiot hyväksyvät ja ottavat käyttöön ensimmäisen alakohdan mukaisia yhteisiä toimia koskevat järjestelyt ja menettelyt kansallisen lakinsa mukaisesti.

3. Valvontaelin, jolle avunantopyyntö on osoitettu, voi kieltäytyä noudattamasta pyyntöä millä hyvänsä seuraavalla perusteella:
- a) pyydetty apu ei ole oikeassa suhteessa valvontaelimen 46 a ja 46 b artiklan mukaisesti toteuttamiin valvontatehtäviin;

- b) valvontaelimellä ei ole toimivaltaa antaa pyydettyä apua;
 - c) pyydetyn avun antaminen olisi ristiriidassa tämän asetuksen kanssa.
4. Edellä 46 e artiklan 1 kohdan mukaisesti perustettu yhteistyöryhmä antaa viimeistään ... päivänä ...kuuta ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] ja sen jälkeen kahden vuoden välein ohjeita tämän artiklan 1 ja 2 kohdassa tarkoitettun keskinäisen avunannon organisatorisista näkökohdista ja menettelyistä.

46 e artikla

Eurooppalaisen digitaalisen identiteetin yhteistyöryhmä

1. Komissio perustaa eurooppalaisen digitaalisen identiteetin yhteistyöryhmän, jäljempänä 'yhteistyöryhmä', luottamuspalveluja, eurooppalaisia digitaalisen identiteetin lompakoita ja ilmoitettuja sähköisen tunnistamisen järjestelmiä koskevan jäsenvaltioiden rajatylittävän yhteistyön ja tietojenvaihdon tukemiseksi ja helpottamiseksi.
2. Yhteistyöryhmä muodostuu jäsenvaltioiden ja komission nimeämistä edustajista. Yhteistyöryhmän puheenjohtajana toimii komissio. Komissio huolehtii yhteistyöryhmän sihteeristön tehtävistä.
3. Asiaankuuluvien sidosryhmien edustajia voidaan tapauskohtaisesti kutsua osallistumaan yhteistyöryhmän kokouksiin ja sen työskentelyyn tarkkailijoina.

4. ENISA kutsutaan osallistumaan tarkkailijana yhteistyöryhmän työskentelyyn, kun yhteistyöryhmä vaihtaa näkemyksiä, parhaita käytäntöjä ja tietoja asiaankuuluvista kyberturvallisuuskohdista, kuten tietoturvaloukkauksista ilmoittamisesta, ja kun käsitellään kyberturvallisuussertifikaattien käyttöä tai standardeja.
5. Yhteistyöryhmällä on seuraavat tehtävät:
 - a) neuvojen vaihtaminen ja yhteistyö komission kanssa digitaalisen identiteetin lompakoiden, sähköisen tunnistamisen menetelmien ja luottamuspalvelujen alalla kehitteillä olevien toimintapoliittisten aloitteiden osalta;
 - b) tarvittaessa neuvojen antaminen komissiolle tämän asetuksen nojalla hyväksyttävien täytäntöönpanosäädösehdotusten ja delegoitujen säädösehdotusten varhaisessa valmisteluvaiheessa;
 - c) valvontaelinten tukemiseksi tämän asetuksen säännösten täytäntöönpanossa yhteistyöryhmä
 - i) vaihtaa parhaita käytäntöjä ja tietoja tämän asetuksen säännösten täytäntöönpanosta;
 - ii) arvioi digitaalisen identiteetin lompakon, sähköisen tunnistamisen ja luottamuspalvelujen alan kehitystä;
 - iii) järjestää eri puolilta unionia tulevien asiaankuuluvien sidosryhmien kanssa yhteiskokouksia, joissa keskustellaan yhteistyöryhmän toteuttamista toimista ja kerätään näkemyksiä esiin nousevista toimintapoliittisista haasteista;

- iv) vaihtaa ENISAn tuella näkemyksiä, parhaita käytäntöjä ja tietoja eurooppalaisiin digitaalisen identiteetin lompakoihin, sähköisen tunnistamisen järjestelmiin ja luottamuspalveluihin liittyvistä asiaankuuluvista kyberturvallisuusnäkökohdista;
 - v) vaihtaa parhaita käytäntöjä 5 e ja 10 artiklassa tarkoitettujen tietoturvaloukkausten ilmoittamista ja yhteisiä toimenpiteitä koskevien toimintaperiaatteiden kehittämistä ja täytäntöönpanosta;
 - vi) järjestää yhteisiä kokouksia direktiivin (EU) 2022/2555 14 artiklan 1 kohdan nojalla perustetun verkko- ja tietoturva-alan yhteistyöryhmän kanssa asiaankuuluvien tietojen vaihtamiseksi luottamuspalveluja ja sähköistä tunnistamista koskevien kyberuhkien, poikkeamien, haavoittuvuuksien, tietoisuutta lisäävien aloitteiden, koulutuksen, harjoitusten ja taitojen, valmiuksien kehittämisen, standardien ja teknisten eritelmien valmiuksien sekä standardien ja teknisten eritelmien osalta;
 - vii) keskustee valvontaelimen pyynnöstä yksittäisistä 46 d artiklassa tarkoitettua keskinäistä avunantoa koskevista pyynnöistä;
 - viii) helpottaa valvontaelinten välistä tietojenvaihtoa antamalla opastusta 46 d artiklassa tarkoitetun keskinäisen avunannon organisatorisista näkökohdista ja menettelyistä;
- d) tämän asetuksen soveltamisalaan kuuluvien ilmoitettavien sähköisen tunnistamisen järjestelmien vertaisarviointien järjestäminen.

6. Jäsenvaltioiden on varmistettava nimettyjen edustajiensa tuloksellinen ja tehokas yhteistyö yhteistyöryhmässä.
7. Komissio vahvistaa viimeistään ... päivänä ...kuussa ... [12 kuukautta tämän muutosasetuksen voimaantulopäivästä] tarvittavat menettelytavat tämän artiklan 5 kohdan d alakohdassa tarkoitetun jäsenvaltioiden välisen yhteistyön helpottamiseksi antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”;

48) muutetaan 47 artikla seuraavasti:

a) korvataan 2 ja 3 kohta seuraavasti:

- ”2. Siirretään komissiolle 17 päivästä syyskuuta 2014 määräämättömäksi ajaksi 5 c artiklan 7 kohdassa, 24 artiklan 4 b kohdassa ja 30 artiklan 4 kohdassa tarkoitettu valta antaa delegoituja säädöksiä.
3. Euroopan parlamentti tai neuvosto voi milloin tahansa peruuttaa 5 c artiklan 7 kohdassa, 24 artiklan 4 b kohdassa ja 30 artiklan 4 kohdassa tarkoitetun säädösvallan siirron. Peruuttamispäätöksellä lopetetaan tuossa päätöksessä mainittu säädösvallan siirto. Peruuttaminen tulee voimaan sitä päivää seuraavana päivänä, jona sitä koskeva päätös julkaistaan *Euroopan unionin virallisessa lehdessä*, tai jonakin myöhempänä, kyseisessä päätöksessä mainittuna päivänä. Peruuttamispäätös ei vaikuta jo voimassa olevien delegoitujen säädösten pätevyYTEEN.”;

b) korvataan 5 kohta seuraavasti:

”5. Edellä olevien 5 c artiklan 7 kohdan, 24 artiklan 4 b kohdan tai 30 artiklan 4 kohdan nojalla annettu delegoitu säädös tulee voimaan ainoastaan, jos Euroopan parlamentti tai neuvosto ei ole kahden kuukauden kuluessa siitä, kun asianomainen säädös on annettu tiedoksi Euroopan parlamentille ja neuvostolle, ilmaissut vastustavansa sitä tai jos sekä Euroopan parlamentti että neuvosto ovat ennen mainitun määräajan päättymistä ilmoittaneet komissiolle, että ne eivät vastusta säädöstä. Euroopan parlamentin tai neuvoston aloitteesta tätä määräaikaä jatketaan kahdella kuukaudella.”;

49) lisätään VI lukuun artikla seuraavasti:

”48 a artikla

Raportointivaatimukset

1. Jäsenvaltioiden on varmistettava, että eurooppalaisten digitaalisen identiteetin lompakoiden ja hyväksytyjen luottamuspalvelujen toiminnasta kerätään tilastotietoja, kun ne on tarjottu niiden alueella.
2. Edellä 1 kohdan mukaisesti kerättyihin tilastotietoihin on sisällyttävä seuraavat:
 - a) niiden luonnollisten ja oikeushenkilöiden lukumäärä, joilla on voimassa oleva eurooppalainen digitaalisen identiteetin lompakko;
 - b) niiden palvelujen tyyppi ja lukumäärä, jotka hyväksyvät eurooppalaisen digitaalisen identiteetin lompakon käytön;

- c) luottaviin osapuoliin ja hyväksytyihin luottamuspalveluihin liittyvien käyttäjävalitusten ja kuluttajansuoja- tai tietosuojapoikkeamien lukumäärä;
- d) tiivistelmäraportti, joka sisältää tiedot eurooppalaisen digitaalisen identiteetin lompakon käytön estävistä poikkeamista;
- e) tiivistelmä merkittävistä tietoturvapoikkeamista, tietoturvaloukkauksista ja niiden kohteeksi joutuneista eurooppalaisten digitaalisen identiteetin lompakkojen tai hyväksytyjen luottamuspalvelujen käyttäjistä.

- 3. Edellä 2 kohdassa tarkoitettujen tilastotiedot on julkaistava avoimesti ja yleisesti käytetyssä koneellisesti luettavassa muodossa.
- 4. Jäsenvaltioiden on toimitettava komissiolle kunkin vuoden 31 päivään maaliskuuta mennessä kertomus 2 kohdan mukaisesti kerätyistä tilastoista.”;

50) korvataan 49 artikla seuraavasti:

”49 artikla

Uudelleentarkastelu

- 1. Komissio tarkastelee uudelleen tämän asetuksen soveltamista ja antaa viimeistään ... päivänä ...kuuta ... [24 kuukautta tämän muutosasetuksen voimaantulopäivästä] Euroopan parlamentille ja neuvostolle kertomuksen. Kertomuksessa komissio arvioi erityisesti, olisiko tämän asetuksen tai sen tiettyjen säännösten, mukaan lukien erityisesti 5 c artiklan 5 kohdan säännösten, soveltamisalaa asianmukaista muuttaa, ottaen huomioon tämän asetuksen soveltamisesta saatu kokemus sekä tekninen, markkinoihin liittyvä ja oikeudellinen kehitys. Kertomukseen liitetään tarvittaessa tämän asetuksen muuttamista koskeva ehdotus.

2. Edellä 1 kohdassa tarkoitettuun kertomukseen on sisällyttävä arvio tämän asetuksen soveltamisalaan kuuluvien ilmoitettujen sähköisen tunnistamisen menetelmien ja eurooppalaisten digitaalisen identiteetin lompakoiden saatavuudesta, turvallisuudesta ja käytettävyydestä sekä arvio siitä, onko kaikille yksityisille verkkopalvelujen tarjoajille, jotka käyttävät kolmannen osapuolen tarjoamia sähköisen tunnistamisen palveluja käyttäjien todentamista varten, hyväksyttävä ilmoitettujen sähköisen tunnistamisen menetelmien ja eurooppalaisten digitaalisen identiteetin lompakon käyttö.
3. Komissio antaa viimeistään ... päivänä ...kuuta ... [kuusi vuotta tämän muutosasetuksen voimaantulopäivästä] ja sen jälkeen neljän vuoden välein Euroopan parlamentille ja neuvostolle kertomuksen edistymisestä tämän asetuksen tavoitteiden saavuttamisessa.”;

51) korvataan 51 artikla seuraavasti:

”51 artikla

Siirtymätoimenpiteet

1. Turvallisia allekirjoituksen luontivälineitä, joiden vaatimustenmukaisuus on määritetty direktiivin 1999/93/EY 3 artiklan 4 kohdan mukaisesti, pidetään edelleen tämän asetuksen mukaisina hyväksytyinä sähköisen allekirjoituksen luontivälineinä ... päivään ...kuuta ... [36 kuukautta tämän muutosasetuksen voimaantulopäivästä].
2. Direktiivin 1999/93/EY mukaisesti luonnollisille henkilöille myönnettyjä hyväksytyjä varmenteita pidetään tämän asetuksen mukaisina sähköisten allekirjoitusten hyväksytyinä varmenteina ... päivään ...kuuta ... [24 kuukautta tämän muutosasetuksen voimaantulopäivästä].

3. Niiden hyväksytyjen luottamuspalvelun tarjoajien hallinnointia, jotka eivät ole hyväksytyjä luottamuspalveluja hyväksytyjen sähköisen allekirjoituksen ja leiman etäluontivälineiden hallinnointia varten 29 a ja 39 a artiklan mukaisesti tarjoavia hyväksytyjä luottamuspalvelun tarjoajia, saadaan suorittaa ilman, että niiden on tarvetta saada hyväksytyt asema näiden hallinnointipalvelujen tarjoamiseksi ... päivään ...kuuta ... [24 kuukautta tämän muutosasetuksen voimaantulopäivästä].
 4. Hyväksytyjen luottamuspalvelun tarjoajien, joille on myönnetty hyväksytyt asema tämän asetuksen nojalla ennen ... päivää ...kuuta ... [tämän muutosasetuksen voimaantulopäivä], on toimitettava valvontaelimelle vaatimustenmukaisuuden arviointiraportti, jossa vahvistetaan 24 artiklan 1, 1 a ja 1 b kohdan noudattaminen, mahdollisimman pian ja joka tapauksessa viimeistään ... päivänä ...kuuta ... [24 kuukautta tämän muutosasetuksen voimaantulopäivästä].”;
- 52) muutetaan liitteet I–IV tämän asetuksen liitteiden I–IV mukaisesti;
- 53) lisätään uudet liitteet V, VI ja VII tämän asetuksen liitteiden V, VI ja VII mukaisesti.

2 artikla
Voimaantulo

Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Brysselissä

Euroopan parlamentin puolesta
Puhemies

Neuvoston puolesta
Puheenjohtaja

LIITE I

Korvataan asetuksen (EU) N:o 910/2014 liitteessä I oleva i alakohta seuraavasti:

- ”i) tieto hyväksytyt varmenteen voimassaolon tilasta tai niiden palvelujen sijainti, joista sen voi selvittää;”.
-

LIITE II

Poistetaan asetuksen (EU) N:o 910/2014 liitteestä II kohta 3 ja 4.

LIITE III

Korvataan asetuksen (EU) N:o 910/2014 liitteessä III oleva i alakohta seuraavasti:

- ”i) tieto hyväksytyt varmenteen voimassaolon tilasta tai niiden palvelujen sijainti, joista sen voi selvittää;”.
-

LIITE IV

Muutetaan asetuksen (EU) N:o 910/2014 liite IV seuraavasti:

1) korvataan c alakohta seuraavasti:

”c) luonnollisten henkilöiden osalta: ainakin sen henkilön nimi, jolle varmenne on myönnetty, tai pseudonyymi; jos käytetään pseudonyymiä, asiasta on ilmoitettava selvästi;

c a) oikeushenkilöiden osalta: sitä oikeushenkilöä, jolle varmenne on myönnetty, yksiselitteisesti edustava yksilöivä tietokokonaisuus ja ainakin sen oikeushenkilön nimi, jolle varmenne on myönnetty, ja tapauksen mukaan rekisterinumero virallisissa rekistereissä olevassa muodossa;”;

2) korvataan j alakohta seuraavasti:

”j) tieto hyväksytyt varmenteen voimassaolon tilasta tai niiden palvelujen sijainti, joista sen voi selvittää.”.

LIITE V

”LIITE V

HYVÄKSYTTYJÄ SÄHKÖISIÄ ATTRIBUUTTITODISTUKSIA KOSKEVAT VAATIMUKSET

Hyväksytyjen sähköisten attribuuttitodistusten on sisällettävä:

- a) tieto, ainakin automaattiseen tietojenkäsittelyyn soveltuvassa muodossa, siitä, että todistus on myönnetty hyväksyttynä sähköisenä attribuuttitodistuksena;
- b) tietokokonaisuus, joka yksiselitteisesti edustaa hyväksytyyn sähköisen attribuuttitodistuksen myöntävää hyväksytyä luottamuspalvelun tarjoajaa ja sisältää ainakin tiedon jäsenvaltiosta, johon tarjoaja on sijoittautunut, ja
 - i) oikeushenkilön osalta: nimi ja tarvittaessa rekisterinumero virallisissa rekistereissä olevassa muodossa,
 - ii) luonnollisen henkilön osalta: henkilön nimi;
- c) tietokokonaisuus, joka yksiselitteisesti edustaa tahoa, johon todistetut attribuutit viittaavat; jos käytetään pseudonyymiä, asiasta on ilmoitettava selvästi;
- d) todistettu attribuutti tai todistetut attribuutit, tarvittaessa mukaan lukien tiedot, jotka ovat tarpeen kyseisten attribuuttien kattavuuden määrittämiseksi;

- e) tiedot todistuksen voimassaoloajan alkamisesta ja päättymisestä;
 - f) todistuksen tunniste, jonka on oltava kyseisen hyväksytyyn luottamuspalvelun tarjoajan osalta yksilöivä, ja tarvittaessa tieto todistusjärjestelmästä, jonka osa attribuuttitodistus on;
 - g) myöntävän hyväksytyyn luottamuspalvelun tarjoajan hyväksyty sähköinen allekirjoitus tai hyväksyty sähköinen leima;
 - h) sijainti, josta g kohdassa tarkoitettua hyväksytyä sähköistä allekirjoitusta tai hyväksytyä sähköistä leimaa tukeva varmenne on saatavilla veloitusetta;
 - i) tieto hyväksytyyn todistuksen voimassaolon tilasta tai niiden palvelujen sijainti, joista sen voi selvittää.”.
-

LIITE VI

”LIITE VI

ATTRIBUUTTIEN VÄHIMMÄISLUETTELO

Tämän asetuksen 45 e artiklan mukaisesti jäsenvaltioiden on varmistettava, että toteutetaan toimenpiteitä, joiden avulla sähköisten attribuuttitodistusten hyväksytyt luottamuspalvelun tarjoajat voivat käyttäjän pyynnöstä tarkastaa seuraavien attribuuttien aitouden sähköisin menetelmin suoraan asianomaisesta virallisesta lähteestä kansallisen tasolla tai sellaisten nimettyjen välittäjien kautta, jotka on tunnustettu kansallisella tasolla, unionin oikeuden tai kansallisen lainsäädännön mukaisesti ja jos nämä attribuutit perustuvat julkisen sektorin virallisiin lähteisiin:

1. Osoite
2. Ikä
3. Sukupuoli
4. Siviilisäätty
5. Perheen koostumus
6. Kansallisuus tai kansalaisuus
7. Tutkinto, tutkintonimike ja koulutustodistukset

8. Ammattipätevyys, ammattinimikkeet ja toimiluvat
 9. Valtuudet ja valtuutukset edustaa luonnollisia tai oikeushenkilöitä
 10. Julkiset luvat
 11. Oikeushenkilöiden osalta taloudelliset ja yritystiedot.”.
-

LIITE VII

”LIITE VII

VIRALLISESTA LÄHTEESTÄ VASTAAVAN JULKISEN ELIMEN MYÖNTÄMÄÄ TAI SEN PUOLESTA MYÖNNETTYÄ SÄHKÖISTÄ ATTRIBUUTTITODISTUSTA KOSKEVAT VAATIMUKSET

Virallisesta lähteestä vastaavan julkisen elimen myöntämän tai sen puolesta myönnetyn sähköisen attribuuttitodistuksen on sisällettävä seuraavat:

- a) vähintään automaattiseen käsittelyyn soveltuvassa muodossa oleva ilmoitus siitä, että todistus on myönnetty sähköisenä attribuuttitodistuksena, jonka on myöntänyt virallisesta lähteestä vastaava julkinen elin tai joka on myönnetty sen puolesta;
- b) tietokokonaisuus, joka yksiselitteisesti edustaa sähköisen attribuuttitodistuksen myöntävää julkista elintä, mukaan lukien vähintään jäsenvaltio, johon kyseinen julkinen elin on sijoittautunut, ja sen nimi ja tarvittaessa sen rekisterinumero virallisissa rekistereissä olevassa muodossa;
- c) tietokokonaisuus, joka yksiselitteisesti edustaa tahoa, johon todistetut attribuutit viittaavat; jos käytetään pseudonyymiä, asiasta on ilmoitettava selvästi;
- d) todistettu attribuutti tai todistetut attribuutit, tarvittaessa mukaan lukien tiedot, jotka ovat tarpeen kyseisten attribuuttien kattavuuden määrittämiseksi;

- e) tiedot todistuksen voimassaoloajan alkamisesta ja päättymisestä;
 - f) todistuksen tunniste, jonka on oltava kyseisen myöntävän julkisen elimen osalta yksilöivä, ja tarvittaessa tieto todistusjärjestelmästä, jonka osa attribuuttitodistus on;
 - g) myöntävän elimen hyväksytty sähköinen allekirjoitus tai hyväksytty sähköinen leima;
 - h) sijainti, josta g kohdassa tarkoitettua hyväksyttyä sähköistä allekirjoitusta tai hyväksyttyä sähköistä leimaa tukeva varmenne on saatavilla veloitusetta;
 - i) tieto todistuksen voimassaolon tilasta tai niiden palvelujen sijainti, joista sen voi selvittää.”.
-