Euroopan unionin neuvosto

Bryssel, 25. marraskuuta 2022
(OR. en)

14959/22

Toimielinten välinen asia:
2021/0136(COD)

LIMITE

TELECOM 473
COMPET 919
MI 844
DATAPROTECT 321
JAI 1497
CODEC 1774

ILMOITUS

Lähettäjä:	Pysyvien edustajien komitea (Coreper I)
Vastaanottaja:	Neuvosto
Ed. asiak. nro:	14344/22
Kom:n asiak. nro:	9471/21
Asia:	Ehdotus Euroopan parlamentin ja neuvoston asetukseksi asetuksen (EU) N:o 910/2014 muuttamisesta eurooppalaisen digitaalisen identiteetin kehyksen vahvistamisen osalta – Yleisnäkemys

I JOHDANTO

1. Komissio hyväksyi ehdotuksen asetukseksi eurooppalaisesta digitaalisesta identiteetistä (**eurooppalainen sähköinen tunnistamisjärjestelmä**) 3. kesäkuuta 2021[1]. Aloitteella muutetaan vuonna 2014 annettua eIDAS-asetusta[2], jolla luotiin tarvittava perusta palvelujen turvalliselle saatavuudelle ja liiketoimien suorittamiselle verkossa ja rajojen yli EU:ssa.

[1] Asiak. 9471/21.
[2] Asetus (EU) N:o 910/2014.

2. SEUT 114 artiklaan perustuva ehdotus edellyttää, että jäsenvaltiot ottavat käyttöön eurooppalaisen digitaalisen identiteetin lompakon, joka on osa ilmoitettua sähköisen tunnistamisen järjestelmää ja perustuu yhteisiin teknisiin normeihin ja edellyttää pakollista sertifiointia. Tarvittavan teknisen rakenteen luomiseksi, tarkistetun asetuksen täytäntöönpanon nopeuttamiseksi, suuntaviivojen antamiseksi jäsenvaltioille ja hajanaisuuden välttämiseksi ehdotukseen liitettiin suositus unionin yhteisen välineistön kehittämisestä.

3. Ehdotetulla asetuksella pyritään varmistamaan, että ihmisille ja yrityksille on yleisesti saatavilla turvallinen ja luotettava sähköinen tunnistautuminen ja todentaminen matkapuhelimella olevan henkilökohtaisen digitaalisen lompakon kautta.

II KÄSITTELY MUISSA TOIMIELIMISSÄ

1. Euroopan parlamentissa ehdotus annettiin teollisuus-, tutkimus- ja energiavaliokunnan (ITRE) käsiteltäväksi. Kolmelta valiokunnalta pyydettiin lausuntoa: sisämarkkina- ja kuluttajansuojavaliokunta (IMCO), oikeudellisten asioiden valiokunta (JURI) ja kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunta (LIBE). Asian esittelijä on Romana Jerković (S&D, Kroatia). ITRE-valiokunta ei ole vielä hyväksynyt mietintöään.

2. Euroopan talous- ja sosiaalikomiteaa pyydettiin 15. heinäkuuta 2021 antamaan ehdotuksesta lausunto. Se annettiin 20. lokakuuta 2021. Euroopan alueiden komitea antoi oma-aloitteisesti lausuntonsa ehdotuksesta 12. lokakuuta 2021.

3. Euroopan tietosuojavaltuutettu julkaisi virallisia kommentteja ehdotuksesta 28. heinäkuuta 2021.

III KÄSITTELY NEUVOSTOSSA

1. Neuvostossa ehdotusta on käsitelty televiestintä- ja tietoyhteiskuntatyöryhmässä, jossa keskustelut alkoivat Portugalin puheenjohtajakaudella kesäkuussa 2021. Ehdotuksen tarkastelua televiestintä- ja tietoyhteiskuntatyöryhmässä jatkettiin Slovenian puheenjohtajakaudella ja ensimmäinen käsittely saatiin onnistuneesti päätökseen 15. marraskuuta 2021.

2. Puheenjohtajavaltio Ranska esitti **ensimmäisen kompromissiehdotuksensa** 15. helmikuuta ja 5. huhtikuuta, ja **toisesta kompromissiehdotuksesta** keskusteltiin 23. toukokuuta ja 9. kesäkuuta. Televiestintä- ja tietoyhteiskuntatyöryhmässä 19. heinäkuuta 2022 käydyn periaatekeskustelun yhteydessä puheenjohtajavaltio Tšekki esitteli – Ranskan puheenjohtajakaudella tehdyn työn pohjalta – tärkeimmät avoinna olevat korkean tason kysymykset ja pyysi valtuuskuntia esittämään parhaaksi katsomansa vaihtoehdot, jotta toisen kompromissiehdotuksen asiaankuuluvat osat voitaisiin muotoilla niiden mukaisesti uudelleen. Tarkistettu versio johti **kolmanteen kompromissiehdotukseen**, jonka puheenjohtajavaltio Tšekki esitti televiestintä- ja tietoyhteiskuntatyöryhmässä 5. ja 8. syyskuuta. Lisäkeskusteluilla ja niihin liittyvillä mukautuksilla päästiin syvemmän tason lähentymiseen useimmista avoinna olevista kysymyksistä.

3. **Neljäs kompromissiehdotus**, joka esiteltiin valtuuskunnille televiestintä- ja tietoyhteiskuntatyöryhmän kokouksessa 28. syyskuuta, paljasti kuitenkin jäsenvaltioiden näkemyksissä edelleen eroja, jotka liittyvät erityisesti keskeiseen kysymykseen eurooppalaiselle digitaalisen identiteetin lompakolle valittavasta varmuustasosta. Jotkin niistä jäsenvaltioista, joissa on jo käytössä kansallinen sähköisen tunnistamisen järjestelmä, ovat alun perin hyväksyneet sen ja sittemmin käyttäneet sitä varmuustasolla ”korotettu”, kun taas nykyisessä sähköistä tunnistamista koskevassa ehdotuksessa edellytetään varmuustasoa ”korkea”. Koska puheenjohtajavaltio Tšekki on tietoinen siitä, että suuri määrä sähköisen tunnistamisen menetelmiä on annettu käyttöön korotetulla varmuustasolla joissakin jäsenvaltioissa, se on ehdottanut lisäksi mekanismia, jolla helpotetaan käyttäjien asiakassuhteen perustamista ja edistetään näin eurooppalaisten digitaalisen identiteetin lompakoiden käyttöönottoa. Säännöksen mukaan käyttäjät voivat kirjautua eurooppalaiseen digitaalisen identiteetin lompakkoon hyödyntämällä olemassa olevia kansallisia sähköisen tunnistamisen menetelmiä, joiden varmuustaso on korotettu, muiden asiakassuhteen perustamisen etämenettelyjen kanssa, jotka yhdessä täyttävät korkean varmuustason vaatimukset. Teknisiin ja toiminnallisiin eritelmiin sovelletaan täytäntöönpanolainsäädäntöä, ja vaatimustenmukaisuus on varmennettava.

4. **Viidettä kompromissiehdotusta** käsiteltiin televiestintä- ja tietoyhteiskuntatyöryhmän kokouksessa 25. lokakuuta. Puheenjohtajavaltio Tšekki esitteli tekstiin tehdyt vähäiset muutokset televiestintä- ja tietoyhteiskuntatyöryhmän kokouksessa 8. marraskuuta 2022 ja laati valtuuskunnilta saatujen lisähuomautusten ja muotoiluehdotusten perusteella **kompromissiehdotuksen lopullisen version** toimitettavaksi pysyvien edustajien komitealle.

5. Pysyvien edustajien komitea tarkasteli kompromissiehdotusta 18. marraskuuta ja **päätti yksimielisesti sen toimittamisesta muutoksitta liikenne-, televiestintä- ja energianeuvostolle (televiestintä) yleisnäkemyksen muodostamiseksi** sen 6. joulukuuta 2022 pidettävässä istunnossa.

IV KOMPROMISSIEHDOTUKSEN KESKEISET OSATEKIJÄT

1. Eurooppalainen digitaalisen identiteetin lompakko

Yksi eurooppalaista digitaalisen identiteetin lompakkoa, jäljempänä ’lompakko’, koskevan komission ehdotuksen tärkeimmistä poliittisista tavoitteista on tarjota kansalaisille ja muille asukkaille, sellaisina kuin heidät on määritelty kansallisessa lainsäädännössä, yhdenmukaistettu eurooppalainen digitaalisen identiteetin väline, joka perustuu eurooppalaisen digitaalisen identiteetin lompakon käsitteeseen. Kansallisten järjestelmien mukaisena, korkean varmuustason sähköisen tunnistamisen menetelmänä käyttöön annettava lompakko olisi itsenäinen sähköisen tunnistamisen menetelmä, joka perustuu siihen, että jäsenvaltiot antavat käyttöön henkilötunnistetietoja ja lompakon.

2. Eurooppalaisten digitaalisen identiteetin lompakoiden varmuustaso

Varmuustasojen olisi luonnehdittava sähköisen tunnistamisen menetelmän luotettavuuden astetta henkilön henkilöllisyyden toteamisessa ja siten tarjottava varmuus siitä, että henkilö, joka väittää omaavansa tietyn henkilöllisyyden, on tosiasiassa henkilö, jolle kyseinen henkilöllisyys on osoitettu. Työryhmäkokouksissa ja pysyvien edustajien komiteassa 14. lokakuuta käydyissä keskusteluissa saadun laajan kannatuksen perusteella lompakko on annettava käyttöön sellaisen sähköisen tunnistamisen järjestelmän puitteissa, joka täyttää korkean varmuustason. Lisäksi **6 a artiklaan** on lisätty erityinen säännös käyttäjien asiakassuhteen perustamisesta. Tämän muutoksen tarkoituksena on ottaa huomioon niiden jäsenvaltioiden huolenaiheet, joissa merkittävä määrä kansallisia sähköisen tunnistamisen menetelmiä on jo annettu käyttöön korotetulla varmuustasolla. Säännös mahdollistaa sen, että käyttäjä voi käyttää kansallisia sähköisen tunnistamisen menetelmiään yhdessä muiden asiakassuhteen perustamisen etämenettelyjen kanssa, jotta on mahdollista todistaa

henkilöllisyys korkealla varmuustasolla ja sitten saada käyttöön lompakko. Koska sähköistä tunnistamista koskeva asetusehdotus perustuu kyberturvallisuuden sertifiointijärjestelmiin, joiden pitäisi saada aikaan tasoltaan yhdenmukainen luottamus eurooppalaisten digitaalisen identiteetin lompakoiden turvallisuuteen, myös salausaineiston turvalliseen tallentamiseen odotetaan sovellettavan kyberturvallisuussertifiointia. Puheenjohtajavaltio on sen vuoksi ehdottanut kyseisiä korkean varmuustason saavuttamisen teknisiä edellytyksiä käsittelevää uutta **johdanto-osan 10 b kappaletta**, joka antaa mahdollisuuden seurantaprosessiin eurooppalaisten digitaalisen identiteetin lompakoiden toteutuksen yhteydessä.

3. Luottavien osapuolten ilmoitukset

3.1 Asetuksen **6 b artikla**, joka koskee luottavien osapuolten ilmoituksia, on muotoiltu uudelleen. Pääsääntöisesti ilmoitusmenettelyn, jolla luottava osapuoli ilmoittaa aikeestaan käyttää lompakkoa, olisi oltava kustannustehokas ja oikeassa suhteessa riskiin sekä sillä olisi varmistettava, että luottava osapuoli toimittaa ainakin lompakkoon todentautumiseen tarvittavat tiedot. Oletusarvoisesti vaaditaan vain vähimmäistiedot, ja ilmoitusta varten olisi voitava käyttää automatisoituja tai yksinkertaisia itseraportointimenettelyjä.

3.2 Erityinen järjestelmä voi kuitenkin olla tarpeen alakohtaisten vaatimusten vuoksi, kuten erityisten henkilötietoryhmien käsittelyyn sovellettavien vaatimusten vuoksi. Sen vuoksi on otettu käyttöön tätä koskeva säännös, jonka tarkoituksena on kattaa tapaukset, joissa edellytetään tiukempaa rekisteröinti- tai lupamenettelyä. Jos sitä vastoin unionin oikeudessa tai kansallisessa lainsäädännössä ei aseteta erityisiä vaatimuksia lompakon avulla tarjottaviin tietoihin pääsylle, jäsenvaltiot voivat vapauttaa kyseiset luottavat osapuolet velvollisuudesta ilmoittaa aikeestaan käyttää lompakoita.

4. Sertifiointi

4.1 Asetuksessa olisi edistettävä ja hyödynnettävä asiaankuuluvien ja olemassa olevien kyberturvallisuusasetuksen sertifiointijärjestelmien tai niiden osien käyttöä sekä velvoitettava niiden käyttöön sen sertifioimiseksi, että lompakot tai niiden osat ovat sovellettavien kyberturvallisuusvaatimusten mukaisia. Näin ollen kyberturvallisuusasetuksen kehystä sovelletaan täysimääräisesti, myös kyberturvallisuusasetuksessa säädettyä kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten välistä vertaisarviointimekanismia. Jotta sähköistä tunnistamista koskeva asetus ja kyberturvallisuusasetus olisivat mahdollisimman yhdenmukaiset keskenään, jäsenvaltiot nimeävät julkisia ja yksityisiä elimiä, jotka on akkreditoitu sertifioimaan lompakko kyberturvallisuusasetuksessa säädetyn mukaisesti.

4.2 Lisäksi komissiota kannustetaan antamaan ENISAlle tehtäväksi kehittää ja hyväksyä lompakon kyberturvallisuussertifiointia varten erityinen kyberturvallisuusasetuksen mukainen järjestelmä. Siihen saakka kunnes tällainen järjestelmä on kehitetty, lompakon sertifioinnin perusmenetelmänä käytetään kyberturvallisuusasetuksen nojalla julkaistua yhteisiin kriteereihin perustuvaa eurooppalaista kyberturvallisuuden sertifiointijärjestelmää. Muiden kuin kyberturvallisuuteen liittyvien vaatimusten osalta, erityisesti lompakon muita toiminnallisia ja operatiivisia näkökohtia koskevien vaatimusten osalta, on laadittava luettelo eritelmistä, menettelyistä ja viitestandardeista. Sertifiointi koskee näitä vaatimuksia.

5. Lompakon tarjoamisen toteutusaika

Jäsenvaltioiden antamien ohjeiden perusteella on ehdotettu, että 24 kuukauden toteutusaika lasketaan **6 a artiklan 11 kohdassa** ja **6 c artiklan 4 kohdassa** tarkoitettujen täytäntöönpanosäädösten hyväksymisestä.

6. Maksut

Asetuksen **6 a artiklan 6 a kohdassa** ja vastaavassa johdanto-osan kappaleessa on selvennetty, että lompakoiden käyttöön antamisen, niiden todentamistarkoituksissa tapahtuvan käytön ja niiden peruuttamisen olisi oltava luonnollisille henkilöille maksuttomia. Lukuun ottamatta tapauksia, joissa lompakoita käytetään todentamiseen, lompakon käyttöön perustuvat palvelut voivat aiheuttaa kustannuksia, esimerkiksi sähköisten attribuuttitodistusten antaminen lompakolle.

7. Pääsy laitteisto- ja ohjelmisto-ominaisuuksiin, mukaan lukien turvatekijä

Puheenjohtajavaltio on ehdottanut säätämistä sellaisesta nimenomaisesta yhteydestä asetuksen (EU) 2022/1925 kanssa, jolla varmistetaan pääsy laitteisto- ja ohjelmisto-ominaisuuksiin osana portinvartijoiden tarjoamia ydinalustapalveluja. Uudessa **12 b artiklassa** selvennetään, että lompakoiden tarjoajat ja ilmoitettujen sähköisen tunnistamisen menetelmien käyttöön antajat, jotka toimivat kaupallisessa tai ammatillisessa ominaisuudessa, ovat digimarkkinasäädöksen asiaa koskevassa määritelmässä tarkoitettuja portinvartijoiden yrityskäyttäjiä. Johdanto-osan kappaleeseen on lisätty sanamuoto havainnollistamaan yhteydestä digimarkkinasäädökseen aiheutuvia vaikutuksia, nimittäin sitä, että portinvartijat olisi velvoitettava maksutta varmistamaan tehokas yhteentoimivuus samojen käyttöjärjestelmän, laitteiston tai ohjelmiston ominaisuuksien kanssa, jotka ovat saatavilla tai joita käytetään sen omien oheis- ja tukipalvelujen tarjoamisessa, sekä varmistamaan pääsy näihin ominaisuuksiin yhteentoimivuustarkoituksissa.

8. Julkisten elinten vaihtoehtoiset mahdollisuudet myöntää sähköisiä attribuuttitodistuksia

Hyväksyttyjen sähköisten attribuuttitodistusten myöntäminen hyväksyttyjen tarjoajien toimesta on säilytetty, mukaan lukien jäsenvaltioiden velvollisuus varmistaa, että attribuutit voidaan tarkistaa virallisesta lähteestä julkisella sektorilla. Tämän lisäksi on otettu käyttöön mahdollisuus, että virallisesta lähteestä vastaava julkisen sektorin elin tai nimetty julkisen sektorin elin, joka toimii virallisesta lähteestä vastaavan julkisen sektorin elimen puolesta, voi myöntää lompakolle suoraan sähköisen attribuuttitodistuksen, jolla on samat oikeusvaikutukset kuin hyväksytyllä sähköisellä attribuuttitodistuksella, edellyttäen, että tarvittavat vaatimukset täyttyvät. Ehdotus on otettu huomioon uudessa **45 a** ja **45 da artiklassa** sekä **liitteessä VII**.

9. Tietueiden yhteensovittaminen

Alkuperäinen **11 a artiklan** otsikko on muutettu ”Tietueiden yhteensovittamiseksi”, koska tämä vastaa paremmin säännöksen tavoitetta. Keskustelun perusteella lompakoiden osalta on säilytetty yksilöivän ja pysyvän tunnisteen käsite. Sitä koskevassa määritelmässä selvennetään, että tunniste voi koostua useiden kansallisten ja alakohtaisten tunnisteiden yhdistelmästä, kunhan se palvelee tarkoitustaan. Siinä todetaan nimenomaisesti, että tietueiden yhteensovittamista voidaan helpottaa hyväksytyllä sähköisellä attribuuttitodistuksella. Lisäksi **11 a artiklaan** on sisällytetty suojalauseke, jonka mukaan jäsenvaltioiden on varmistettava henkilötietojen suoja ja estettävä käyttäjien profilointi. Viime kädessä jäsenvaltioiden on luottavina osapuolina varmistettava tietueiden yhteensovittaminen.

VI PÄÄTELMÄ

1. Edellä olevan perusteella neuvostoa pyydetään

   – tarkastelemaan tämän ilmoituksen liitteessä olevaa kompromissitekstiä,

   – vahvistamaan liikenne-, televiestintä- ja energianeuvoston istunnossa (televiestintä) 6. joulukuuta 2022 yleisnäkemys eurooppalaista digitaalista identiteettiä koskevasta asetusehdotuksesta (eurooppalainen sähköinen tunnistamisjärjestelmä).

_____

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS

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 lainsäätämisjärjestyksessä hyväksyttäväksi säädökseksi on toimitettu kansallisille parlamenteille,

ottavat huomioon Euroopan talous- ja sosiaalikomitean lausunnon[3],

noudattavat tavallista lainsäätämisjärjestystä,

sekä katsovat seuraavaa:

(1) Komission 19 päivänä helmikuuta 2020 antamassa tiedonannossa ”Euroopan digitaalista tulevaisuutta rakentamassa”[4] ilmoitetaan Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 tarkistamisesta sen tehokkuuden parantamiseksi, sen hyötyjen laajentamiseksi yksityiselle sektorille ja luotettavien digitaalisten identiteettien edistämiseksi kaikille eurooppalaisille.

[3] EUVL C , , s. .
[4] COM/2020/67 final.

(2) Eurooppa-neuvosto kehotti 1 ja 2 päivänä lokakuuta 2020 antamissaan päätelmissä[5] komissiota ehdottamaan unionin laajuisen suojatun julkisen sähköisen tunnistamisjärjestelmän kehyksen 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) Maaliskuun 9 päivänä 2021 annetussa komission tiedonannossa ”2030 digitaalinen kompassi: eurooppalainen lähestymistapa digitaalista vuosikymmentä varten”[6] asetetaan tavoitteeksi unionin kehys, joka johtaa vuoteen 2030 mennessä sellaisen luotettavan, käyttäjän hallitseman tunnistuksen laajamittaiseen käyttöönottoon, jonka avulla jokainen käyttäjä voi hallita omaa toimintaansa ja läsnäoloaan verkossa.

(4) Omaksumalla yhdenmukaisempi lähestymistapa digitaaliseen tunnistamiseen voitaisiin vähentää riskejä ja kustannuksia, joita aiheutuu toisistaan poikkeavien kansallisten ratkaisujen käytöstä johtuvasta nykyisestä hajanaisuudesta, ja vahvistaa sisämarkkinoita antamalla kansalaisille, muille kansallisessa lainsäädännössä määritellyille asukkaille ja yrityksille mahdollisuus tunnistautua verkossa helpolla ja yhdenmukaisella tavalla kaikkialla unionissa. Eurooppalainen digitaalisen identiteetin lompakko tarjoaa luonnollisille henkilöille ja oikeushenkilöille kaikkialla unionissa yhdenmukaistetun sähköisen tunnistamisen menetelmän, jonka avulla nämä voivat todentaa ja jakaa henkilöllisyyteensä liittyviä tietoja. Kaikilla olisi oltava julkisten ja yksityisten palvelujen turvallinen käyttömahdollisuus, joka perustuu parannettuun luottamuspalvelujen ekosysteemiin ja varmennettuihin henkilöllisyystodistuksiin ja attribuuttitodistuksiin, kuten kaikkialla unionissa laillisesti tunnustettuun ja hyväksyttyyn yliopistotutkintoon. Eurooppalaisessa digitaalisen identiteetin kehyksessä pyritään siirtymään pelkästään kansallisten digitaalisten identiteettiratkaisujen käytöstä Euroopan tasolla voimassa oleviin sähköisiin attribuuttitodistuksiin. Sähköisten attribuuttitodistusten tarjoajilla olisi oltava selkeät ja yhdenmukaiset säännöt, ja julkishallintojen olisi voitava luottaa tietyssä muodossa oleviin sähköisiin asiakirjoihin.

---

5 https://www.consilium.europa.eu/fi/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/

6 COM/2021/118 final/2.

(4 a) Useat jäsenvaltiot ovat toteuttaneet ja suurelta osin käyttävät sähköisen tunnistamisen menetelmiä, jotka unionissa toimivat palveluntarjoajat nykyisin hyväksyvät. Lisäksi on tehty investointeja sekä kansallisiin että rajatylittäviin ratkaisuihin nykyisen eIDAS-asetuksen perusteella, mukaan lukien eIDAS-solmukohtien yhteentoimivuuden tekninen infrastruktuuri. Jotta voidaan taata 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 ja hyödyntävän käytössä olevaa eIDAS-infrastruktuuria Euroopan ja jäsenvaltioiden tasolla.

(5) Eurooppalaisten yritysten kilpailukyvyn tukemiseksi verkkopalvelujen tarjoajien olisi voitava käyttää kaikkialla unionissa tunnustettuja digitaalisia identiteettiratkaisuja riippumatta siitä, missä jäsenvaltiossa ne on tarjottu, ja hyötyä näin yhdenmukaisesta eurooppalaisesta lähestymistavasta luottamukseen, turvallisuuteen ja yhteentoimivuuteen. Sekä käyttäjien että palveluntarjoajien olisi voitava hyötyä siitä, että sähköisille attribuuttitodistuksille annetaan sama oikeudellinen arvo kaikkialla unionissa.

(6) Tämän asetuksen täytäntöönpanon yhteydessä tapahtuvaan henkilötietojen käsittelyyn sovelletaan asetusta (EU) 2016/679[7]. Sen vuoksi tässä asetuksessa olisi säädettävä erityisistä suojatoimista, joilla estetään sähköisen tunnistamisen menetelmien ja sähköisten attribuuttitodistusten tarjoajia yhdistämästä muista palveluista saatuja henkilötietoja tämän asetuksen soveltamisalaan kuuluviin palveluihin liittyviin henkilötietoihin. Eurooppalaisten digitaalisen identiteetin lompakoiden tarjoamiseen liittyvät henkilötiedot olisi pidettävä loogisesti erillään kaikista muista lompakon käyttöön antajan hallussa olevista tiedoista. Tämä asetus ei estä eurooppalaisten digitaalisen identiteetin lompakoiden käyttöön antajia soveltamasta henkilötietojen suojaa parantavia teknisiä lisätoimenpiteitä, kuten lompakoiden tarjoamiseen liittyvien henkilötietojen fyysistä erottamista kaikista muista lompakon käyttöön antajan hallussa olevista tiedoista.

---

[7] 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).

(7) On tarpeen määritellä yhdenmukaistetut edellytykset sellaisen kehyksen vahvistamiseksi jäsenvaltioiden tarjoamia eurooppalaisia digitaalisen identiteetin lompakoita varten, joka antaisi kaikille unionin kansalaisille ja muille kansallisessa lainsäädännössä määritellyille asukkaille mahdollisuuden jakaa turvallisesti henkilöllisyyteensä liittyviä tietoja käyttäjäystävällisellä ja helppokäyttöisellä tavalla käyttäjän yksinomaisessa valvonnassa. Näiden tavoitteiden saavuttamiseksi käytettäviä tekniikoita olisi kehitettävä siten, että tavoitteena on mahdollisimman korkeatasoinen turvallisuus, yksityisyys ja käyttäjäystävällisyys sekä laaja käytettävyys. Jäsenvaltioiden olisi varmistettava, että kaikilla niiden kansalaisilla ja asukkailla on yhtäläinen mahdollisuus käyttää digitaalista tunnistamista.

(8) Jotta voidaan varmistaa, että luottavat osapuolet voivat luottaa eurooppalaisten digitaalisen identiteetin lompakoiden käyttöön, ja suojata käyttäjää arkaluonteisten tietojen laittomalta käytöltä, luottavat osapuolet olisi rekisteröitävä osana ilmoitusmenettelyä. Luottaviin osapuoliin sovellettavien ilmoitusvaatimusten olisi useimmissa tapauksissa perustuttava siihen, että luottavan osapuolen todentamiseksi eurooppalaisen digitaalisen identiteetin lompakkoon olisi toimitettava vain rajattu määrä tietoja. Vaatimusten olisi myös mahdollistettava automatisoitujen tai yksinkertaisten itseraportointimenettelyjen käyttö, mukaan lukien se, että jäsenvaltiot luottavat olemassa oleviin rekistereihinsä ja käyttävät niitä. Samaan aikaan kansallisella tai unionin tasolla voi olla olemassa arkaluonteisten tietojen luokkia varten erityisiä järjestelmiä, joissa voidaan asettaa luottaville osapuolille tiukempia rekisteröinti- ja lupavaatimuksia, jotta voidaan estää henkilöllisyystietojen laiton käyttö tällaisissa tapauksissa. Muissa käyttötapauksissa luottavat osapuolet voidaan vapauttaa velvollisuudesta ilmoittaa aikomuksestaan käyttää eurooppalaista digitaalisen identiteetin lompakkoa esimerkiksi silloin, kun oikeus tarkistaa tietyt attribuutit ei edellytä tai salli luottavan osapuolen todentamista sähköisesti. Näissä henkilöön liittyvissä skenaarioissa käyttäjä pystyy yleensä tunnistamaan luottavan osapuolen asiayhteyden ansiosta, esimerkiksi ollessaan vuorovaikutuksessa autonvuokraajan tai apteekkarin kanssa. Ilmoitusmenettelyn on tarkoitus perustua alakohtaiseen unionin tai kansalliseen lainsäädäntöön, koska sen avulla voidaan ottaa huomioon erilaisia käyttötapauksia, jotka voivat vaihdella rekisteröintivaatimusten, toimintatavan (verkossa / verkon ulkopuolella) tai niiden laitteiden todentamisvaatimuksen osalta, jotka pystyvät toimimaan yhdessä eurooppalaisen digitaalisen identiteetin lompakon kanssa. Tarkastusta, joka koskee luottavan osapuolen eurooppalaisen digitaalisen identiteetin lompakon käyttöä, ei olisi velvoitettava täytäntöönpantavaksi eurooppalaisen digitaalisen identiteetin lompakon tasolla.

(9) 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. Lompakot voivat palvella myös julkishallintojen, kansainvälisten järjestöjen ja unionin toimielinten, elinten, laitosten ja virastojen institutionaalisia tarpeita, sanotun kuitenkaan rajoittamatta kansalaisten ja asukkaiden tunnistamiseen liittyviä jäsenvaltioiden oikeuksia. Verkon ulkopuolinen käyttö olisi tärkeää monilla terveydenhuollon kaltaisilla aloilla, joilla palveluja tarjotaan usein henkilökohtaisen vuorovaikutuksen kautta. Myös sähköisissä lääkemääräyksissä olisi voitava luottaa QR-koodeihin tai vastaaviin teknologioihin aitouden todentamiseksi. Eurooppalaisissa digitaalisen identiteetin lompakoissa, joilta edellytetään korkeaa varmuustasoa, 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 hyväksyttyjä sähköisiä allekirjoituksia ja leimoja, jotka hyväksytään kaikkialla EU:ssa. Jotta kansalaisille ja yrityksille kaikkialla EU:ssa voidaan tuottaa yksinkertaistamisesta ja kustannussäästöistä koituvia hyötyjä, myös mahdollistamalla edustusvaltuudet ja sähköiset valtuutukset, jäsenvaltioiden olisi tarjottava yhteisiin standardeihin perustuvia eurooppalaisia digitaalisen identiteetin lompakoita saumattoman yhteentoimivuuden ja korkean turvallisuustason varmistamiseksi. 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 olisi perustuttava kansalaisten, muiden asukkaiden tai oikeushenkilöiden oikeudelliseen identiteettiin. Luottamusta eurooppalaisiin digitaalisen identiteetin lompakoihin parantaisi se, että niitä tarjoavien osapuolten edellytetään toteuttavan asianmukaisia teknisiä ja organisatorisia toimenpiteitä sen varmistamiseksi, että turvallisuuden taso on oikeassa suhteessa luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuviin riskeihin asetuksen (EU) 2016/679 mukaisesti. Eurooppalaisten digitaalisen identiteetin lompakoiden käyttöön antamisen, todentamistarkoituksessa tapahtuvan käytön ja peruuttamisen on oltava maksutonta luonnollisille henkilöille. Lompakon käyttöön perustuvat palvelut voivat aiheuttaa kustannuksia, jotka liittyvät esimerkiksi sähköisten attribuuttitodistusten myöntämiseen lompakolle.

(9 a) 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. Tämän tavoitteen saavuttamiseksi jäsenvaltiot voivat säätää oikeudellisista ja organisatorisista toimenpiteistä, joilla joustavuutta lisätään eurooppalaisten digitaalisen identiteetin lompakoiden käyttöön antajien 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. Tämä ei saisi millään tavoin haitata tässä asetuksessa säädettyjen eurooppalaisten digitaalisen identiteetin lompakoiden ydintoimintojen tarjoamista eikä antaa olemassa oleville kansallisille ratkaisuille etusijaa eurooppalaisiin digitaalisen identiteetin lompakoihin nähden. Koska nämä lisätoiminnot menevät tätä asetusta pidemmälle, niihin ei sovelleta tässä asetuksessa vahvistettuja säännöksiä, jotka koskevat eurooppalaisten digitaalisen identiteetin lompakoiden rajatylittävää käyttöä.

(10) Korkeatasoisen tietosuojan, turvallisuuden ja luotettavuuden saavuttamiseksi tässä asetuksessa olisi vahvistettava yhdenmukaistettu kehys, jossa esitetään yksityiskohtaisesti eurooppalaisiin digitaalisen identiteetin lompakoihin sovellettavat yhteiset eritelmät ja vaatimukset. Jäsenvaltioiden nimeämien akkreditoitujen vaatimustenmukaisuuden arviointilaitosten olisi varmennettava, että eurooppalaiset digitaalisen identiteetin lompakot ovat näiden vaatimusten mukaisia. Sertifioinnin olisi perustuttava erityisesti asiaankuuluviin asetuksen (EU) 2019/881[8] nojalla perustettuihin eurooppalaisiin kyberturvallisuuden sertifiointijärjestelmiin tai niiden osiin siltä osin kuin ne kattavat eurooppalaisiin digitaalisen identiteetin lompakoihin sovellettavat kyberturvallisuusvaatimukset. Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käytön on tarkoitus luoda yhdenmukainen luottamus eurooppalaisten digitaalisen identiteetin lompakoiden turvallisuuteen riippumatta siitä, missä päin unionia niitä tarjotaan. Eurooppalaisten digitaalisen identiteetin lompakoiden kyberturvallisuussertifioinnin olisi perustuttava kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten tehtävään, joka on valvoa ja seurata, ovatko niiden lainkäyttöalueella toimivien vaatimustenmukaisuuden arviointilaitosten myöntämät sertifikaatit asiaankuuluvien eurooppalaisten kyberturvallisuusjärjestelmien mukaisia. Samaten sertifioinnissa olisi myös tarvittaessa hyödynnettävä asetuksessa (EU) 2019/881 määriteltyjä standardeja ja teknisiä eritelmiä. Tällaisia eritelmiä voidaan käyttää viimeisintä kehitystä edustavina asiakirjoina asetuksen (EU) 2019/881 mukaisissa asiaankuuluvissa kyberturvallisuuden sertifiointijärjestelmissä määritetyllä tavalla. Jos asetuksen (EU) 2019/881 nojalla perustetut asiaankuuluvat eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät eivät kata lompakon turvallisuutta edistävien asiaankuuluvien palvelujen tai menettelyjen sertifiointia, asianmukaiset järjestelmät olisi luotava asetuksen (EU) 2019/881 III osaston mukaisesti. Eurooppalaisten digitaalisen identiteetin lompakoiden sertifiointia varten olisi perustettava yhteinen ja yhdenmukaistettu järjestelmä sen arvioimiseksi, ovatko ne tässä asetuksessa säädettyjen yhteisten eritelmien ja vaatimusten mukaisia, lukuun ottamatta kyberturvallisuuteen ja tietosuojaan liittyviä eritelmiä ja vaatimuksia, jotka kattavat erityisesti toiminnalliset ja operatiiviset näkökohdat. Tämän sertifioinnin osalta olisi luottamuksen ja avoimuuden korkean tason varmistamiseksi otettava käyttöön mekanismeja ja menettelyjä, joilla pyritään edistämään jäsenvaltioiden välistä vertaisoppimista ja yhteistyötä sertifiointielinten sekä niiden myöntämien sertifikaattien ja sertifiointiraporttien seurannassa ja tarkastelussa. Tällainen vertaisoppimismekanismi ei saisi rajoittaa asetuksen (EU) 2016/679 ja asetuksen (EU) 2019/881 soveltamista. Asetuksen (EU) 2016/679 mukainen lompakon sertifiointi on vapaaehtoinen väline muiden sellaisten välineiden joukossa, joita voidaan käyttää osoittamaan asetuksessa (EU) 2016/679 säädettyjen vaatimusten noudattaminen sellaisina kuin niitä sovelletaan eurooppalaisiin digitaalisen identiteetin lompakoihin ja niiden tarjoamiseen Euroopan kansalaisille.

---

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

(10 a) Kansalaisten ja asukkaiden asiakassuhteen perustamista eurooppalaisen digitaalisen identiteetin lompakon osalta olisi helpotettava käyttämällä sähköisen tunnistamisen menetelmiä, jotka on myönnetty korkealla varmuustasolla. Korotetulla varmuustasolla myönnettyjä sähköisen tunnistamisen menetelmiä olisi käytettävä ainoastaan tapauksissa, joissa yhdenmukaistetut tekniset ja toiminnalliset eritelmät, joissa käytetään korotetulla varmuustasolla myönnettyjä sähköisen tunnistamisen menetelmiä yhdessä muiden täydentävien henkilöllisyyden todentamismenetelmien kanssa, mahdollistavat tässä asetuksessa säädettyjen korkeaa varmuustasoa koskevien vaatimusten täyttymisen. Tällaisten täydentävien menetelmien tai toimenpiteiden olisi oltava luotettavia ja helppokäyttöisiä käyttäjien kannalta, ja ne voisivat perustua mahdollisuuteen käyttää asiakassuhteen perustamisen etämenettelyjä, hyväksyttyjä varmenteita, joita tuetaan hyväksytyillä allekirjoituksilla, hyväksyttyjä sähköisiä attribuuttitodistuksia tai niiden yhdistelmää. Jotta voidaan varmistaa eurooppalaisten digitaalisen identiteetin lompakoiden riittävä käyttöönotto, täytäntöönpanosäädöksissä olisi vahvistettava yhdenmukaistetut tekniset ja toiminnalliset eritelmät käyttäjien asiakassuhteen perustamiseksi sähköisen tunnistamisen menetelmiä käyttäen, mukaan lukien korotetulla varmuustasolla myönnetyt menetelmät.

(10 b) Tämän asetuksen tavoitteena on tarjota käyttäjälle täysin mobiili, turvallinen ja käyttäjäystävällinen eurooppalainen digitaalisen identiteetin lompakko. Eurooppalaiset digitaalisen identiteetin lompakot voivat siirtymätoimenpiteenä siihen saakka, kunnes saatavilla on sertifioituja väärinkäytöltä suojattuja ratkaisuja, kuten käyttäjien laitteissa olevia turvatekijöitä, käyttää salausaineiston ja muiden arkaluonteisten tietojen suojaamiseksi sertifioituja ulkoisia turvatekijöitä tai ilmoitettuja kansallisia ratkaisuja, joiden varmuustaso on korkea, osoittaakseen, että asetuksen asiaankuuluvia vaatimuksia lompakon varmuustason osalta noudatetaan. Edellä mainitun siirtymätoimenpiteen käyttö olisi rajattava tapauksiin, joissa edellytetään korkeaa varmuustasoa, kuten käyttäjän asiakassuhteen perustaminen lompakkoon ja todentamisen tekeminen korkeaa varmuustasoa edellyttäviin palveluihin. Eurooppalaisten digitaalisen identiteetin lompakoiden ei pitäisi edellyttää edellä mainitun siirtymätoimenpiteen käyttöä, kun todentaminen tehdään korotettua varmuustasoa edellyttäviin palveluihin. Tämä asetus ei saisi rajoittaa sertifioidun ulkoisen turvatekijän myöntämistä ja käyttöä koskevien kansallisten edellytysten soveltamista, jos kyseinen siirtymätoimenpide perustuu siihen.

(11) Eurooppalaisten digitaalisen identiteetin lompakoiden olisi varmistettava todentamiseen käytettävien henkilötietojen korkein tietosuoja- ja turvallisuustaso riippumatta siitä, tallennetaanko kyseiset tiedot paikallisesti vai pilvipohjaisiin ratkaisuihin, ottaen huomioon erilaiset riskitasot. Biometristen tietojen käsittely todentamistekijänä käyttäjän vahvan todentamisen yhteydessä on yksi tunnistusmenetelmistä, jotka antavat korkean luottamustason erityisesti silloin, kun niitä käytetään yhdessä muiden todentamistekijöiden kanssa. Koska biometriset tiedot ovat henkilön ainutlaatuisia ominaisuuksia, biometristen tietojen käsittely on sallittua ainoastaan asetuksen (EU) 2016/679 9 artiklan 2 kohdassa säädettyjen poikkeusten nojalla, ja se edellyttää asianmukaisia suojatoimia, jotka ovat oikeassa suhteessa siihen riskiin, jonka tällainen käsittely saattaa aiheuttaa luonnollisten henkilöiden oikeuksille ja vapauksille.

(11 a) Eurooppalaisten digitaalisen identiteetin lompakoiden toiminnan olisi oltava läpinäkyvää ja mahdollistettava todennettavissa oleva henkilötietojen käsittely. Tätä varten jäsenvaltioita kannustetaan luovuttamaan eurooppalaisten digitaalisen identiteetin lompakoiden sellaisten ohjelmistokomponenttien lähdekoodi, jotka liittyvät henkilötietojen ja oikeushenkilöiden tietojen käsittelyyn. Tällaisten lähdekoodien luovuttaminen auttaa yhteiskuntaa, myös käyttäjiä ja kehittäjiä, ymmärtämään sen toimintaa. Tämä voi myös lisätä käyttäjien luottamusta lompakon ekosysteemiin ja edistää lompakoiden turvallisuutta antamalla kenelle tahansa mahdollisuuden ilmoittaa koodien haavoittuvuuksista ja virheistä. Tämä kannustaa toimittajia toimittamaan ja ylläpitämään erittäin turvallista tuotetta. Lisäksi jäsenvaltioita kannustetaan tarvittaessa asettamaan lähdekoodi saataville avoimen lähdekoodin lisenssillä. Avoimen lähdekoodin lisenssin ansiosta yhteiskunta, käyttäjät ja kehittäjät mukaan luettuina, voi muuttaa lähdekoodia ja käyttää sitä uudelleen.

(12) Sen varmistamiseksi, että eurooppalainen digitaalisen identiteetin kehys on avoin innovoinnille ja tekniikan kehitykselle ja pystyy mukautumaan tulevaisuuden vaatimuksiin, jäsenvaltioita olisi kannustettava 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 toimintaympäristön pitäisi edistää eurooppalaisten pienten ja keskisuurten yritysten, startup-yritysten ja yksittäisten innovoijien ja tutkijoiden osallisuutta.

(13) Asetuksella (EU) 2019/1157[9] henkilökorttien turvallisuutta lisätään parannetuilla turvaominaisuuksilla elokuuhun 2021 mennessä. Jäsenvaltioiden olisi harkittava mahdollisuutta ilmoittaa näistä turvaominaisuuksista sähköisen tunnistamisen järjestelmien yhteydessä sähköisen tunnistamisen menetelmien rajatylittävän saatavuuden laajentamiseksi.

(14) 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 910/2014 mukaisina kansallisina sähköisen tunnistamisen järjestelminä.

(15) Nykyisten ilmoitus- ja vertaisarviointimenettelyjen virtaviivaistaminen estää epäyhtenäiset lähestymistavat erilaisten ilmoitettujen sähköisen tunnistamisen järjestelmien arviointiin ja helpottaa luottamuksen rakentamista jäsenvaltioiden välillä. Uusien yksinkertaisempien mekanismien pitäisi edistää jäsenvaltioiden yhteistyötä niiden ilmoittamien sähköisen tunnistamisen järjestelmien turvallisuuden ja yhteentoimivuuden alalla.

(16) Jäsenvaltioiden pitäisi hyötyä uusista joustavista välineistä, joilla varmistetaan tämän asetuksen ja asiaa koskevien täytäntöönpanosäädösten vaatimusten noudattaminen. Tämän asetuksen olisi annettava jäsenvaltioille mahdollisuus käyttää akkreditoitujen vaatimustenmukaisuuden arviointilaitosten tekemiä raportteja ja arviointeja, kuten asetuksen (EU) 2019/881 nojalla unionin tasolla perustettavissa sertifiointijärjestelmissä edellytetään, tukeakseen väitteitään siitä, että järjestelmät tai niiden osat ovat tässä asetuksessa vahvistettujen ilmoitettujen sähköisen tunnistamisen järjestelmien yhteentoimivuutta ja turvallisuutta koskevien vaatimusten mukaisia.

---

[9] 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).

(17 a) Jäsenvaltioiden myöntämien tai eurooppalaisen digitaalisen identiteetin lompakon tuottamien yksilöivien ja pysyvien tunnisteiden käyttö yhdessä henkilön tunnistetietojen käytön kanssa on olennaisen tärkeää sen varmistamiseksi, että käyttäjän henkilöllisyys voidaan todentaa erityisesti julkisella sektorilla ja silloin, kun siitä on säädetty kansallisessa tai unionin lainsäädännössä. Tällä asetuksella olisi varmistettava, että eurooppalainen digitaalisen identiteetin lompakko voi tarjota mekanismin tietueiden yhteensovittamista, myös käyttämällä hyväksyttyjä sähköisiä attribuuttitodistuksia, ja yksilöivien ja pysyvien tunnisteiden henkilön tunnistetietoihin sisällyttämistä varten. Yksilöivä ja pysyvä tunniste voi koostua joko yhdestä tai useammasta tunnistetiedosta, joka voi olla alakohtainen, kunhan käyttäjä voidaan sen avulla tunnistaa yksiselitteisesti kaikkialla unionissa. Eurooppalaisen digitaalisen identiteetin lompakon olisi myös tarjottava mekanismi, joka sallii tiettyä luottavaa osapuolta koskevien erityisten tunnisteiden käytön tapauksissa, joissa kansallisessa tai unionin lainsäädännössä edellytetään yksilöivän ja pysyvän tunnisteen käyttöä. Tietueiden yhteensovittamisen sekä yksilöivien ja pysyvien tunnisteiden käytön helpottamiseksi tarjotulla mekanismilla olisi kaikissa tapauksissa varmistettava, että käyttäjää suojataan henkilötietojen väärinkäytöltä tämän asetuksen ja sovellettavan unionin lainsäädännön, erityisesti asetuksen (EU) 2016/679, mukaisesti, mukaan lukien eurooppalaisen digitaalisen identiteetin lompakon käyttöön liittyvän profiloinnin ja seurannan riskiltä.

(17 aa) On olennaisen tärkeää ottaa huomioon käyttäjien tarpeet ja lisätä siten eurooppalaisten digitaalisen identiteetin lompakoiden kysyntää. Saatavilla olisi oltava mielekkäitä käyttötapauksia ja verkkopalveluja, jotka perustuvat eurooppalaisiin digitaalisen identiteetin lompakoihin. Käyttäjien käyttömukavuuden lisäämiseksi ja tällaisten palvelujen rajatylittävän saatavuuden varmistamiseksi on tärkeää toteuttaa toimia, joilla edistetään samanlaista lähestymistapaa verkkopalvelujen suunnitteluun, kehittämiseen ja toteuttamiseen kaikissa jäsenvaltioissa. Eurooppalaisiin 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.

(18) Direktiivin (EU) 2019/882[10] mukaisesti vammaisten henkilöiden olisi voitava käyttää eurooppalaisia digitaalisen identiteetin lompakoita, luottamuspalveluja ja niiden tarjoamiseksi tarvittavia loppukäyttäjätuotteita tasavertaisesti muiden käyttäjien kanssa.

(19) Tämän asetuksen ei pitäisi kattaa näkökohtia, jotka liittyvät sellaisten sopimusten tai muiden oikeudellisten velvoitteiden vahvistamiseen ja pätevyyteen, joihin sisältyy kansallisessa tai unionin oikeudessa säädettyjä muotovaatimuksia. Sen ei pitäisi myöskään vaikuttaa kansallisiin muotovaatimuksiin, jotka koskevat julkisia rekistereitä, erityisesti kauppa- ja kiinteistörekistereitä.

(20) Luottamuspalvelujen tarjoaminen ja käyttö on käymässä yhä tärkeämmäksi kansainväliselle kaupalle ja yhteistyölle. EU:n kansainväliset kumppanit ovat luomassa luottamuskehyksiä, jotka ovat saaneet innoituksensa asetuksesta (EU) N:o 910/2014. Tällaisten palvelujen ja niiden tarjoajien tunnustamisen helpottamiseksi täytäntöönpanolainsäädännössä voidaan asettaa edellytykset, joiden täyttyessä kolmansien maiden luottamuskehysten voidaan katsoa vastaavan tässä asetuksessa säädettyä hyväksyttyjä luottamuspalveluja ja niiden tarjoajia koskevaa kehystä. Tällä voidaan täydentää mahdollisuutta unioniin ja kolmansiin maihin sijoittautuneiden luottamuspalvelujen ja niiden tarjoajien vastavuoroiseen tunnustamiseen perussopimuksen 218 artiklan mukaisesti. Vahvistettaessa edellytyksiä, joiden täyttyessä kolmansien maiden luottamuskehysten voitaisiin katsoa vastaavan tässä asetuksessa säädettyä hyväksyttyjen luottamuspalvelujen ja palveluntarjoajien luottamuskehystä, olisi varmistettava myös direktiivin XXXX/XXXX (NIS2-direktiivi) ja asetuksen (EU) 2016/679 asiaankuuluvien säännösten noudattaminen sekä luotettavien luetteloiden käyttö oleellisena tekijänä luottamuksen rakentamisessa.

[10] 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).

(21) Tämän asetuksen olisi perustuttava unionin säädöksiin, joilla varmistetaan kilpailulliset ja oikeudenmukaiset markkinat digitaalialalla. Se perustuu erityisesti asetukseen (EU) 2022/1925, jolla otetaan käyttöön portinvartijoiksi nimettyjä ydinalustapalvelujen tarjoajia koskevat säännöt ja muun muassa kielletään portinvartijoita vaatimasta yrityskäyttäjiä käyttämään tai tarjoamaan portinvartijan tunnistuspalvelua tai varmistamaan yhteentoimivuus sen kanssa niiden palvelujen yhteydessä, joita yrityskäyttäjät tarjoavat kyseisen portinvartijan ydinalustapalveluja käyttäen. Asetuksen (EU) 2022/1925 6 artiklan 7 kohdassa edellytetään, että portinvartijoiden on sallittava yrityskäyttäjille ja oheispalvelujen tarjoajille pääsy samoihin käyttöjärjestelmän, laitteiston tai ohjelmiston ominaisuuksiin, jotka ovat saatavilla tai joita käytetään portinvartijan tarjotessa oheispalveluja, ja varmistettava näiden ominaisuuksien yhteentoimivuus. Digimarkkinasäädöksen 2 artiklan 15 alakohdan mukaan tunnistuspalvelut ovat yksi oheispalvelujen tyyppi. Yrityskäyttäjien ja oheispalvelujen tarjoajien olisi sen vuoksi voitava käyttää tällaisia laitteiston tai ohjelmiston ominaisuuksia, kuten älypuhelimien turvatekijöitä, ja varmistaa yhteentoimivuus niiden kanssa eurooppalaisten digitaalisen identiteetin lompakoiden tai jäsenvaltioiden ilmoittamien sähköisen tunnistamisen menetelmien kautta.

(22) Jotta voidaan virtaviivaistaa luottamuspalvelun tarjoajille asetettuja kyberturvallisuusvelvoitteita ja antaa näille palveluntarjoajille ja niistä vastaaville toimivaltaisille viranomaisille mahdollisuus hyötyä direktiivillä XXXX/XXXX (NIS2-direktiivi) vahvistetusta oikeudellisesta kehyksestä, luottamuspalvelujen edellytetään toteutettavan direktiivin XXXX/XXXX (NIS2-direktiivi) 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 direktiivin XXXX/XXXX (NIS2-direktiivi) 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 XXXX/XXXX [NIS2-direktiivi] mukaisten kyberturvallisuusriskien hallintaa koskevien vaatimusten ja raportointivelvoitteiden olisi katsottava täydentävän tämän asetuksen nojalla luottamuspalvelujen tarjoajille asetettuja vaatimuksia. Direktiivin XXXX/XXXX (NIS2-direktiivi) 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. Mitkään tämän asetuksen mukaiset vaatimukset eivät vaikuta velvoitteeseen ilmoittaa henkilötietojen tietoturvaloukkauksista asetuksen (EU) 2016/679 mukaisesti.

(23) Asianmukaista huomiota olisi kiinnitettävä verkko- ja tietoturvaviranomaisten ja eIDAS-viranomaisten välisen tehokkaan yhteistyön varmistamiseen. Tapauksissa, joissa tämän asetuksen mukainen valvontaelin on eri kuin direktiivin XXXX/XXXX [NIS2-direktiivi] nojalla nimetty toimivaltainen viranomainen, kyseisten viranomaisten olisi tehtävä tiivistä ja oikea-aikaista yhteistyötä vaihtamalla asiaankuuluvia tietoja, jotta voidaan varmistaa tehokas valvonta ja se, että luottamuspalvelun tarjoajat noudattavat tässä asetuksessa ja direktiivissä XXXX/XXXX [NIS2-direktiivi] säädettyjä vaatimuksia. Tämän asetuksen mukaisilla valvontaelimillä olisi erityisesti oltava oikeus pyytää direktiivin XXXXX/XXXX [NIS2-direktiivi] mukaista toimivaltaista viranomaista antamaan hyväksytyn aseman myöntämiseksi tarvittavat tiedot ja toteuttamaan valvontatoimia sen varmistamiseksi, että luottamuspalvelun tarjoajat noudattavat NIS2-direktiivin mukaisia asiaankuuluvia vaatimuksia, tai vaatimaan niitä korjaamaan vaatimusten noudattamatta jättämisen.

(24) 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 yleiseurooppalaisten sähköisten rekisteröityjen jakelupalvelujen tarjoamiseksi. Sen varmistamiseksi, että hyväksyttyä sähköistä rekisteröityä jakelupalvelua käytettäessä tiedot toimitetaan oikealle vastaanottajalle, hyväksyttyjen sähköisten rekisteröityjen jakelupalvelujen olisi varmistettava täysin varmasti vastaanottajan tunnistaminen, kun taas lähettäjän tunnistamiseen riittää korkea luottamustaso. Jäsenvaltioiden olisi kannustettava hyväksyttyjen sähköisten rekisteröityjen jakelupalvelujen tarjoajia varmistamaan, että niiden palvelut ovat yhteentoimivia muiden hyväksyttyjen luottamuspalvelun tarjoajien tarjoamien hyväksyttyjen sähköisten rekisteröityjen jakelupalvelujen kanssa, jotta sähköisesti rekisteröidyt tiedot voidaan siirtää helposti kahden tai useamman hyväksytyn luottamuspalvelun tarjoajan välillä ja jotta oikeudenmukaisia käytäntöjä voidaan edistää sisämarkkinoilla.

(25) Useimmissa tapauksissa kansalaiset ja muut asukkaat eivät voi vaihtaa digitaalisesti valtioiden rajojen yli henkilöllisyyteensä liittyviä tietoja, kuten osoitteita, ikää ja ammattipätevyyttä, ajokortteja ja muita lupia ja maksutietoja, turvallisesti ja korkeatasoisella tietosuojalla.

(26) Olisi oltava mahdollista antaa ja käsitellä luotettavia digitaalisia attribuutteja ja auttaa vähentämään hallinnollista taakkaa antamalla kansalaisille ja muille asukkaille mahdollisuus käyttää niitä yksityisissä ja julkisissa transaktioissaan. 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 sosiaaliturvaa koskevia oikeuksiaan tai tulevia sähköisiä matkustusasiakirjoja rajat ylittävässä yhteydessä.

(27) Jokaisen tahon, joka kerää, luo ja antaa todistettuja attribuutteja, kuten tutkintotodistuksia, lisenssejä ja syntymätodistuksia, olisi voitava toimia sähköisten attribuuttitodistusten tarjoajana. Luottavien osapuolten olisi käytettävä sähköisiä attribuuttitodistuksia paperimuodossa olevia todistuksia vastaavina. Tästä syystä sähköisen attribuuttitodistuksen oikeusvaikutuksia ei pitäisi kieltää sillä perusteella, että se on sähköisessä muodossa tai että se ei täytä hyväksytyn sähköisen attribuuttitodistuksen vaatimuksia. Tätä varten olisi vahvistettava yleiset vaatimukset sen varmistamiseksi, että hyväksytyllä sähköisellä attribuuttitodistuksella on samanlaiset oikeusvaikutukset kuin laillisesti paperimuodossa annetuilla todistuksilla. Näitä vaatimuksia olisi kuitenkin sovellettava rajoittamatta sellaisen unionin tai kansallisen lainsäädännön soveltamista, jossa määritellään muotoa koskevia alakohtaisia lisävaatimuksia, joilla on oikeusvaikutuksia, ja tarvittaessa erityisesti rajoittamatta hyväksytyn sähköisen attribuuttitodistuksen rajatylittävää tunnustamista.

(28) Eurooppalaisten digitaalisen identiteetin lompakoiden laaja saatavuus ja käytettävyys edellyttää, että yksityiset palveluntarjoajat hyväksyvät ne. Yksityisten luottavien osapuolten, jotka tarjoavat palveluja liikenteen, energian, pankki- ja rahoituspalvelujen, sosiaaliturvan, terveydenhuollon, juomaveden, postipalvelujen, digitaalisen infrastruktuurin, koulutuksen tai televiestinnän aloilla, olisi hyväksyttävä eurooppalaisten digitaalisen identiteetin lompakoiden käyttö sellaisten palvelujen tarjoamisessa, joissa kansallisen tai unionin lainsäädännön tai sopimusvelvoitteiden mukaisesti edellytetään käyttäjien vahvaa todentamista. Eurooppalaisen digitaalisen identiteetin lompakon käytön ja hyväksymisen helpottamiseksi olisi otettava huomioon laajalti hyväksytyt toimialan standardit ja eritelmät. Jos asetuksen [digipalvelusäädöksen viite] 25 artiklan 1 kohdassa määritellyt erittäin suuret verkkoalustat vaativat käyttäjien todentamista verkkopalveluihin pääsyä varten, kyseiset alustat olisi velvoitettava hyväksymään eurooppalaisten digitaalisen identiteetin lompakoiden käyttö käyttäjän vapaaehtoisesta pyynnöstä. Käyttäjillä ei pitäisi olla velvollisuutta käyttää lompakkoa päästäkseen yksityisiin palveluihin, mutta jos he haluavat tehdä niin, erittäin suurten verkkoalustojen olisi hyväksyttävä eurooppalainen digitaalinen identiteetin lompakko tätä tarkoitusta varten noudattaen samalla tietojen minimoinnin periaatetta. Tämä on tarpeen, jotta voidaan parantaa käyttäjien suojaa petoksilta ja varmistaa korkeatasoinen tietosuoja, kun otetaan huomioon erittäin suurten verkkoalustojen merkitys, mikä johtuu niiden kattavuudesta, erityisesti palvelun käyttäjien ja taloudellisten transaktioiden lukumääränä ilmaistuna. Unionin tasolla olisi kehitettävä itsesääntelyyn perustuvia käytännesääntöjä, jäljempänä ’käytännesäännöt’, jotta edistettäisiin sähköisen tunnistamisen menetelmien, myös eurooppalaisten digitaalisen identiteetin lompakoiden, laajaa saatavuutta ja käytettävyyttä tämän asetuksen soveltamisalalla. Käytännesäännöillä 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. Käytännesäännöt olisi laadittava 12 kuukauden kuluessa tämän asetuksen hyväksymisestä. Komission olisi arvioitava näiden säännösten tehokkuutta eurooppalaisten digitaalisen identiteetin lompakoiden saatavuuden ja käytettävyyden kannalta 24 kuukauden kuluttua niiden käyttöönotosta.

(29) Valikoiva luovuttaminen tarkoittaa, että tietojen omistajalle annetaan valtuudet luovuttaa vain tietyt laajemman tietokokonaisuuden osat, jotta vastaanottava yhteisö saa ainoastaan tarvittavat tiedot, esimerkiksi jotta käyttäjä voi luovuttaa luottavalle osapuolelle vain käyttäjän pyytämän palvelun tarjoamiseen tarvittavat tiedot. Eurooppalaisen digitaalisen identiteetin lompakon olisi teknisesti mahdollistettava attribuuttien valikoiva luovuttaminen luottaville osapuolille. Tällaiset valikoivasti luovutetut attribuutit voidaan myöhemmin yhdistää ja esittää luottaville osapuolille, myös silloin, kun attribuutit ovat alun perin olleet useissa erillisissä sähköisissä todistuksissa. Tästä ominaisuudesta olisi tultava lompakon perusominaisuus, mikä lisää käyttömukavuutta ja henkilötietojen suojaa, mukaan lukien tietojen minimointi.

(30) Hyväksyttyjen luottamuspalvelun tarjoajien osana hyväksyttyä sähköistä attribuuttitodistusta tarjoamat attribuutit olisi tarkastettava virallisista lähteistä joko suoraan hyväksytyn luottamuspalvelun tarjoajan toimesta tai sellaisten nimettyjen välittäjien kautta, jotka on kansallisen tai unionin 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 hyväksyttyjä sähköisiä attribuuttitodistuksia myöntävät hyväksytyt luottamuspalvelun tarjoajat voivat sen henkilön suostumuksella, jolle todistus on myönnetty, todentaa attribuuttien aitouden virallisten lähteiden perusteella. Asianmukaisiin mekanismeihin voi kuulua erityisten välittäjien tai teknisten ratkaisujen käyttö kansallisen lainsäädännön mukaisesti, mahdollistaen virallisten lähteiden saatavuuden. Sen varmistaminen, että saatavilla on attribuuttien todentamisen virallisista lähteistä mahdollistava mekanismi, helpottaisi hyväksyttyjen sähköisten attribuuttitodistusten hyväksyttyjen luottamuspalvelujen tarjoajien tässä asetuksessa säädettyjen velvoitteiden noudattamista. Liitteessä VI on luettelo attribuuttiluokista, joiden osalta jäsenvaltioiden olisi varmistettava, että toteutetaan toimenpiteitä, jotta sähköisten attribuuttitodistusten hyväksytyt tarjoajat voivat tarkistaa sähköisesti niiden aitouden asianomaisesta virallisesta lähteestä käyttäjän pyynnöstä. Näihin luokkiin kuuluvista attribuuteista olisi sovittava jäsenvaltioiden kanssa.

(31) Turvallisessa sähköisessä tunnistamisessa ja attribuuttitodistusten antamisessa olisi tarjottava rahoituspalvelualalle lisäjoustoa ja -ratkaisuja, jotka mahdollistavat asiakkaiden tunnistamisen ja sellaisten erityisten attribuuttien vaihdon, joita tarvitaan esimerkiksi rahanpesun torjuntaa 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.

(31 a) Jotta voidaan varmistaa sertifiointikäytäntöjen johdonmukaisuus kaikkialla EU:ssa, komission olisi annettava ohjeet hyväksyttyjen sähköisen allekirjoituksen luontivälineiden ja hyväksyttyjen sähköisen leiman luontivälineiden sertifioinnista ja uudelleensertifioinnista, mukaan lukien niiden voimassaolo ja ajalliset rajoitukset. Tämä asetus ei estä jäsenvaltioita sallimasta julkisten tai yksityisten elinten, joilla on sertifioituja hyväksyttyjä sähköisen allekirjoituksen luontivälineitä, jatkaa sertifioinnin voimassaoloa väliaikaisesti, jos saman välineen uudelleensertifiointia ei ole voitu suorittaa laissa määritellyssä määräajassa muusta syystä kuin tietoturvaloukkauksesta tai turvallisuushäiriöstä, sanotun kuitenkaan rajoittamatta sovellettavaa sertifiointikäytäntöä.

(32) Verkkosivustojen todentamispalvelut tarjoavat käyttäjille korkean varmuustason siitä, että verkkosivuston taustalla on aito ja laillinen taho, riippumatta siitä, mitä alustaa sen näyttämiseen käytetään. Nämä palvelut lisäävät luottamusta verkossa asiointiin ja vähentävät verkkopetoksia. Verkkosivustojen todentamispalvelujen käytön olisi oltava vapaaehtoista verkkosivustoille. Jotta verkkosivustojen todentamisesta tulisi kuitenkin keino lisätä luottamusta, parantaa käyttäjän kokemusta ja edistää kasvua sisämarkkinoilla, tässä asetuksessa olisi säädettävä tietoturvaa ja vastuuta koskevista vähimmäisvelvoitteista verkkosivustojen todentamispalvelujen tarjoajien ja niiden palvelujen osalta. Tätä varten verkkoselainten tarjoajien olisi varmistettava tuki verkkosivustojen todentamisen hyväksytyille varmenteille ja yhteentoimivuus niiden kanssa asetuksen (EU) N:o 910/2014 mukaisesti. Niiden olisi tunnustettava verkkosivustojen todentamisen hyväksytyt varmenteet ja sallittava sertifioitujen henkilötietojen esittäminen loppukäyttäjälle selainympäristössä tämän asetuksen mukaisesti vahvistettujen eritelmien perusteella. Verkkosivustojen todentamisen hyväksytyn varmenteen tunnustamisella hyväksytyn luottamuspalvelun tarjoajan myöntämäksi hyväksytyksi varmenteeksi olisi varmistettava, että varmenteeseen sisältyvät henkilötiedot voidaan todentaa ja tarkastaa tämän asetuksen mukaisesti. Tämä ei saisi vaikuttaa verkkoselaimen tarjoajien mahdollisuuteen puuttua merkittäviin vaatimustenvastaisuuksiin, jotka liittyvät tietoturvaloukkauksiin ja eheyden menetyksiin yksittäisten varmenteiden osalta, mikä edistää loppukäyttäjien verkkoturvallisuutta. Kansalaisten suojelun ja verkkosivustojen todentamisen hyväksyttyjen varmenteiden käytön edistämiseksi edelleen jäsenvaltioiden viranomaisten olisi harkittava kyseisten varmenteiden sisällyttämistä verkkosivustoihinsa.

(33) Monet jäsenvaltiot ovat ottaneet käyttöön kansallisia vaatimuksia turvallista ja luotettavaa digitaalista arkistointia tarjoaville palveluille, jotta sähköisiä tietoja ja niihin liittyviä luottamuspalveluja voidaan säilyttää pitkällä aikavälillä. Oikeusvarmuuden, luottamuksen ja yhdenmukaistamisen varmistamiseksi kaikissa jäsenvaltioissa olisi vahvistettava hyväksyttyjä sähköisiä arkistointipalveluja koskeva oikeudellinen kehys, joka perustuu tässä asetuksessa säädettyyn muita luottamuspalveluja koskevaan kehykseen. Kehyksen olisi tarjottava luottamuspalvelun tarjoajille ja käyttäjille tehokas välineistö, jossa huomioidaan sähköisen arkistointipalvelun toiminnalliset vaatimukset sekä selkeät oikeusvaikutukset, kun käytetään hyväksyttyä sähköistä arkistointipalvelua. Näitä säännöksiä olisi sovellettava sähköisesti tuotettuihin asiakirjoihin sekä paperiasiakirjoihin, jotka on skannattu ja digitoitu. Näiden säännösten olisi tarvittaessa mahdollistettava säilytettyjen sähköisten tietojen siirtäminen eri tallennusvälineille tai -muodoille, jotta niiden kestävyyttä ja luettavuutta voidaan jatkaa teknologista luotettavuusaikaa pidemmälle, samalla kun tietojen häviämistä ja muuttumista minimoidaan mahdollisimman paljon. Jos sähköiseen arkistointipalveluun toimitetut sähköiset tiedot sisältävät yhden tai useamman hyväksytyn sähköisen allekirjoituksen tai hyväksytyn sähköisen leiman, palvelun olisi käytettävä menettelyjä ja teknologioita, joilla voidaan pidentää niiden luotettavuutta tällaisten tietojen säilyttämisajan verran, mahdollisesti käyttämällä muita tällä asetuksella vahvistettuja hyväksyttyjä luottamuspalveluja. Säilyttämistä koskevan näytön luomiseen sähköisten allekirjoitusten, sähköisten leimojen tai sähköisten aikaleimojen käytön osalta olisi käytettävä hyväksyttyjä sähköisiä luottamuspalveluja. Siltä osin kuin sähköisiä arkistointipalveluja ei yhdenmukaisteta tällä asetuksella, jäsenvaltiot voivat pitää voimassa tai ottaa käyttöön kyseisiä palveluja koskevia unionin oikeuden mukaisia kansallisia säännöksiä, kuten erityissäännöksiä, joissa sallitaan joitakin poikkeuksia organisaatioon integroitujen palvelujen osalta ja joita käytetään tiukasti kyseisen organisaation ”sisäisissä arkistoissa”. Tässä asetuksessa ei pitäisi tehdä eroa sähköisesti tuotettujen asiakirjojen ja digitoitujen fyysisten asiakirjojen välillä.

(33 a) Kansallisille arkistoille ja muistiorganisaatioille eli organisaatioille, jotka on omistettu asiakirjaperinnön säilyttämiselle yleisen edun vuoksi, annetaan yleensä kansallisen lainsäädännön nojalla valtuudet harjoittaa toimintaansa ja ne eivät välttämättä tarjoa tässä asetuksessa tarkoitettuja luottamuspalveluja. Siltä osin kuin nämä laitokset eivät tarjoa tällaisia palveluja, tämä asetus ei vaikuta niiden toimintaan.

(34) Sähköiset tilikirjat ovat sarja sähköisiä tietoja, joilla varmistetaan tietojen eheys ja kronologisen järjestyksen oikeellisuus. Sähköisten tilikirjojen tarkoituksena on määrittää tietojen kronologinen järjestys, jotta voidaan estää digitaalisen omaisuuden kopiointi ja myynti useille vastaanottajille. Sähköisiä tilikirjoja voidaan käyttää esimerkiksi omistusoikeuden osoittaviin digitaalisiin tallenteisiin, jotka liittyvät maailmanlaajuiseen kauppaan, toimitusketjun rahoitukseen, teollis- ja tekijänoikeuksiin tai sähkön kaltaisiin hyödykkeisiin. Yhdessä muiden teknologioiden kanssa ne voivat edistää ratkaisuja tehokkaampien ja muutosvoimaisempien julkisten palvelujen luomiseksi, kuten sähköinen äänestäminen, tulliviranomaisten rajatylittävä yhteistyö, akateemisten laitosten rajatylittävä yhteistyö tai kiinteistöjen omistusoikeuden kirjaaminen hajautettuihin maarekistereihin. Hyväksytyt sähköiset tilikirjat luovat oikeudellisen olettaman tilikirjan tietojen yksilöllisestä ja oikeellisesta peräkkäisestä kronologisesta järjestyksestä ja eheydestä. Sähköisten tilikirjojen erityisattribuutit eli tietojen peräkkäinen kronologinen järjestys erottaa sähköiset tilikirjat muista luottamuspalveluista, kuten sähköisistä aikaleimoista ja sähköisistä rekisteröidyistä jakelupalveluista. Toisin sanoen sähköisten asiakirjojen aikaleimaaminen tai niiden siirtäminen sähköisten rekisteröityjen jakelupalvelujen avulla ei ilman muita teknisiä tai organisatorisia toimenpiteitä voi riittävällä tavalla estää saman digitaalisen omaisuuden kopiointia ja myyntiä eri osapuolille useammin kuin kerran. Sähköisen tilikirjan laatimis- ja päivittämisprosessi riippuu käytetyn tilikirjan tyypistä (keskitetty tai jaettu).

(35) Sisämarkkinoiden pirstaloitumisen estämiseksi olisi perustettava yleiseurooppalainen oikeudellinen kehys, joka mahdollistaa luottamuspalvelujen rajatylittävän tunnustamisen tietojen tallentamiseksi hyväksyttyihin sähköisiin tilikirjoihin. Sähköisten tilikirjojen luottamuspalvelun tarjoajat olisi valtuutettava varmistamaan tietojen peräkkäinen kirjaaminen tilikirjaan. Tämä asetus ei vaikuta oikeudellisiin velvoitteisiin, joita sähköisten tilikirjojen käyttäjien on mahdollisesti noudatettava unionin ja kansallisen lainsäädännön nojalla. Esimerkiksi käyttötapauksissa, joihin liittyy henkilötietojen käsittelyä, olisi noudatettava asetusta (EU) 2016/679. Kryptovaroihin liittyvien käyttötapausten olisi oltava yhteensopivia kaikkien sovellettavien rahoitussääntöjen kanssa, mukaan lukien esimerkiksi rahoitusmarkkinadirektiivi[11], maksupalveludirektiivi[12], sähköistä rahaa koskeva direktiivi[13], sekä kryptovarojen markkinoita koskevan mahdollisen tulevan lainsäädännön ja rahanpesun torjuntaa koskevien sääntöjen kanssa, jotka voitaisiin sisällyttää varainsiirtoasetukseen[14], ja niissä voitaisiin edellyttää, että kryptovarapalvelun tarjoajat todentavat sähköisen tilikirjan käyttäjien henkilöllisyyden noudattaakseen kansainvälisiä rahanpesun torjuntaa koskevia standardeja.

---

11 Euroopan parlamentin ja neuvoston direktiivi 2014/65/EU, annettu 15 päivänä toukokuuta 2014, rahoitusvälineiden markkinoista sekä direktiivin 2002/92/EY ja direktiivin 2011/61/EU muuttamisesta (EUVL L 173, 12.6.2014, s. 349–496).

12 Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/2366, annettu 25 päivänä marraskuuta 2015, maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/110/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta (EUVL L 337, 23.12.2015, s. 35–127).

13 Euroopan parlamentin ja neuvoston direktiivi 2009/110/EY, annettu 16 päivänä syyskuuta 2009, sähköisen rahan liikkeeseenlaskijalaitosten liiketoiminnan aloittamisesta, harjoittamisesta ja toiminnan vakauden valvonnasta, direktiivien 2005/60/EY ja 2006/48/EY muuttamisesta sekä direktiivin 2000/46/EY kumoamisesta (EUVL L 267, 10.10.2009, s. 7–17).

14 Ks. komission ehdotus, annettu 20 päivänä heinäkuuta 2021, varainsiirtojen ja tiettyjen kryptovarojen siirtojen mukana toimitettavista tiedoista 20 päivänä toukokuuta 2015 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2015/847 uudelleenlaatimisesta (COM/2021/422 final).

(36) Jotta voidaan välttää erilaisista standardeista ja teknisistä rajoituksista johtuva hajanaisuus ja esteet ja varmistaa koordinoitu prosessi ja jotta ei vaaranneta tulevan eurooppalaisen digitaalisen identiteetin kehyksen täytäntöönpanoa, tarvitaan komission, jäsenvaltioiden ja yksityisen sektorin välistä tiivistä ja jäsenneltyä yhteistyötä. Tämän tavoitteen saavuttamiseksi jäsenvaltioiden olisi tehtävä yhteistyötä komission suosituksessa XXX/XXXX[15] [välineistö eurooppalaista digitaalisen identiteetin kehystä koskevaa koordinoitua lähestymistapaa varten] vahvistetuissa puitteissa, jotta voidaan määrittää välineistö eurooppalaista digitaalisen identiteetin kehystä varten. Välineistöön olisi sisällyttävä kattava tekninen arkkitehtuuri ja viitekehys, joukko yhteisiä standardeja ja teknisiä viiteasiakirjoja sekä joukko parhaita käytäntöjä koskevia suuntaviivoja ja kuvauksia, jotka kattavat vähintään kaikki näkökohdat, jotka liittyvät eurooppalaisten digitaalisen identiteetin lompakoiden toimintoihin ja yhteentoimivuuteen, sähköiset allekirjoitukset mukaan luettuina, sekä tässä asetuksessa säädettyyn attribuuttitodistuksia koskevaan hyväksyttyyn luottamuspalveluun. Tässä yhteydessä jäsenvaltioiden olisi myös päästävä sopimukseen eurooppalaisten digitaalisen identiteetin lompakoiden liiketoimintamallin ja maksurakenteen yhteisistä osatekijöistä lompakoiden käyttöönoton helpottamiseksi rajatylittävissä yhteyksissä erityisesti pienissä ja keskisuurissa yrityksissä. Välineistön sisältöä olisi kehitettävä rinnakkain eurooppalaista digitaalisen identiteetin kehystä koskevan keskustelun ja hyväksymisprosessin kanssa ja siinä olisi otettava huomioon niiden tulokset.

(36 a) Jäsenvaltioiden olisi vahvistettava säännöt, jotka koskevat seuraamuksia rikkomuksista, kuten suorista tai epäsuorista käytännöistä, jotka johtavat sekaannukseen ei-hyväksyttyjen ja hyväksyttyjen luottamuspalvelujen välillä tai siihen, että ei-hyväksytyt luottamuspalvelun tarjoajat käyttävät EU:n luotettavuusmerkkiä väärin. EU:n luotettavuusmerkkiä ei pitäisi käyttää tavoin, jotka suoraan tai välillisesti johtavat uskomaan, että tietyn palveluntarjoajan tarjoamat ei-hyväksytyt luottamuspalvelut olisivat hyväksyttyjä.

[15] [Viite lisätään hyväksymisen jälkeen]

(36 b) Tällä asetuksella olisi varmistettava hyväksyttyjen luottamuspalvelujen laadun, luotettavuuden ja turvallisuuden yhdenmukainen taso riippumatta siitä, missä toimintaa harjoitetaan. Hyväksytyn luottamuspalvelun tarjoajan olisi voitava ulkoistaa hyväksytyn luottamuspalvelun tarjoamiseen liittyvät toimensa unionin ulkopuolelle, jos se antaa takeet ja varmistaa, että valvontatoimet ja tarkastukset voidaan panna täytäntöön ikään kuin nämä toimet suoritettaisiin unionissa. Jos asetuksen noudattamista ei voida täysin varmistaa, valvontaelinten olisi voitava hyväksyä oikeasuhtaisia ja perusteltuja toimenpiteitä, mukaan lukien luottamuspalvelulle annetun hyväksytyn aseman peruuttaminen.

(36 c) Kehittyneen ja hyväksyttyyn varmenteeseen perustuvan sähköisen allekirjoituksen pätevyyttä koskevan oikeusvarmuuden varmistamiseksi on tärkeää yksilöidä ne kehittyneen ja hyväksyttyyn varmenteeseen perustuvan sähköisen allekirjoituksen osatekijät, jotka kyseisen allekirjoituksen validoinnin suorittavan luottavan osapuolen olisi arvioitava.

(36 d) Luottamuspalvelujen tarjoajien olisi käytettävä salausalgoritmeja nykyisten parhaiden käytäntöjen mukaisesti ja näiden algoritmien luotettavaa täytäntöönpanoa voidakseen varmistaa luottamuspalvelujensa turvallisuuden ja luotettavuuden.

(36 e) Tässä asetuksessa olisi säädettävä hyväksyttyjen luottamuspalvelun tarjoajien velvollisuudesta todentaa sellaisen luonnollisen henkilön tai oikeushenkilön henkilöllisyys, jolle hyväksytty varmenne on myönnetty, käyttäen EU:ssa yhdenmukaistettuja eri menetelmiä. Tällaiseen menetelmään voi kuulua turvautuminen sähköisen tunnistamisen menetelmiin, jotka täyttävät korotettua varmuustasoa koskevat vaatimukset, yhdistettynä muihin yhdenmukaistettuihin etämenettelyihin, joilla varmistetaan henkilön tunnistamisen korkea luottamustaso.

(36 f) Eurooppalaisten digitaalisen identiteetin lompakoiden käyttöön antajien ja ilmoitettujen sähköisen tunnistamisen menetelmien myöntäjien, jotka toimivat kaupallisessa tai ammatillisessa ominaisuudessa käyttäen portinvartijoiden tarjoamia ydinalustapalveluja tavaroiden ja palvelujen tarjoamiseksi loppukäyttäjille tai näiden tarjoamisen aikana, olisi pidettävä yrityskäyttäjinä asetuksen (EU) 2022/1925 2 artiklan 21 alakohdan mukaisesti. Portinvartijat olisi sen vuoksi velvoitettava varmistamaan maksutta tehokas yhteentoimivuus ja pääsy yhteentoimivuuden varmistamiseksi samoihin käyttöjärjestelmän, laitteiston tai ohjelmiston ominaisuuksiin, jotka ovat saatavilla tai joita käytetään sen omien oheis- ja tukipalvelujen ja laitteistojen tarjoamisessa. Tämän pitäisi antaa eurooppalaisten digitaalisen identiteetin lompakoiden käyttöön antajille ja ilmoitettujen sähköisen tunnistamisen menetelmien myöntäjille mahdollisuus toisiaan vastaavien ominaisuuksien yhteenliittämiselle rajapintojen tai vastaavien ratkaisujen kautta yhtä tehokkaasti kuin portinvartijan omilla palveluilla tai laitteistoilla.

(36 g) Jotta voidaan pitää tämä asetus nykykehityksen mukaisena ja noudattaa sisämarkkinoiden käytäntöjä, komission hyväksymiä delegoituja säädöksiä ja täytäntöönpanosäädöksiä olisi säännöllisesti tarkasteltava uudelleen ja tarvittaessa ajantasaistettava. Näiden päivitysten tarpeellisuuden arvioinnissa olisi otettava huomioon sisämarkkinoilla esiin tulleet uudet teknologiat, käytännöt, standardit tai tekniset eritelmät.

(37) Euroopan tietosuojavaltuutettua on kuultu Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1525[16] 42 artiklan 1 kohdan mukaisesti.

(38) Sen vuoksi asetusta (EU) 910/2014 olisi muutettava,

---

16 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).

OVAT HYVÄKSYNEET TÄMÄN ASETUKSEN:

1 artikla

Muutetaan asetus (EU) 910/2014 seuraavasti:

1) Korvataan 1 artikla seuraavasti:

”Tällä asetuksella pyritään varmistamaan sisämarkkinoiden moitteeton toiminta ja tarjoamaan samalla sähköisen tunnistamisen menetelmien ja luottamuspalvelujen tietoturvan riittävän korkea taso. Tätä varten tässä asetuksessa

aa) säädetään ehdoista, joiden mukaisesti jäsenvaltioiden on tarjottava toisen jäsenvaltion ilmoitetun sähköisen tunnistamisen järjestelmän piiriin kuuluvia luonnollisten henkilöiden ja oikeushenkilöiden sähköisen tunnistamisen menetelmiä ja tunnustettava ne;

ab) vahvistetaan edellytykset, joiden mukaisesti jäsenvaltiot 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, sähköisten allekirjoitusten, sähköisten leimojen ja niiden varmenteiden sähköiselle validoinnille, verkkosivustojen todentamisen varmenteiden sähköiselle validoinnille, sähköisten allekirjoitusten, sähköisten leimojen ja niiden varmenteiden sähköiselle säilyttämiselle, sähköiselle arkistoinnille, sähköisille attribuuttitodistuksille, hyväksytyn sähköisen allekirjoituksen ja leiman etäluontivälineiden hallinnalle ja sähköisille tilikirjoille;”

2) Muutetaan 2 artikla seuraavasti:

a) korvataan 1 kohta seuraavasti:

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

b) korvataan 3 kohta seuraavasti:

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

3) Muutetaan 3 artikla seuraavasti:

X) Korvataan 1 alakohta seuraavasti:

”1. ’sähköisellä tunnistamisella’ prosessia, jossa käytetään tiettyä luonnollista henkilöä, oikeushenkilöä taikka luonnollista henkilöä tai oikeushenkilöä edustavaa luonnollista henkilöä vastaavia yksilöiviä tunnistetietoja sähköisessä muodossa;”

a) korvataan 2 alakohta seuraavasti:

”2. ’sähköisen tunnistamisen menetelmällä’ aineellista ja/tai aineetonta kokonaisuutta, mukaan lukien eurooppalainen digitaalisen identiteetin lompakko, joka sisältää henkilön tunnistetietoja ja jota käytetään verkkopalveluun tai tarvittaessa muualla kuin verkossa toimivaan palveluun liittyvään todentamiseen;”

aa) korvataan 3 alakohta seuraavasti:

”3. ’henkilön tunnistetiedoilla’ tietoja, jotka on annettu unionin tai kansallisen lainsäädännön mukaisesti ja jotka mahdollistavat luonnollisen henkilön, oikeushenkilön taikka luonnollista henkilöä tai oikeushenkilöä edustavan luonnollisen henkilön henkilöllisyyden toteamisen;”

b) korvataan 4 alakohta seuraavasti:

”4. ’sähköisen tunnistamisen järjestelmällä’ sähköiseen tunnistamiseen liittyvää järjestelmää, jonka puitteissa sähköisen tunnistamisen menetelmiä myönnetään luonnollisille henkilöille, oikeushenkilöille taikka luonnollista henkilöä tai oikeushenkilöä edustaville luonnollisille henkilöille;”

ba) korvataan 5 alakohta seuraavasti:

”5. ’todentamisella’ sähköistä prosessia, joka mahdollistaa luonnollisen henkilön tai oikeushenkilön sähköisen tunnistamisen tai sähköisessä muodossa olevien tietojen alkuperän ja eheyden vahvistamisen;”

bb) lisätään 5 a alakohta seuraavasti:

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

c) korvataan 14 alakohta seuraavasti:

”14. ’sähköisen allekirjoituksen varmenteella’ sähköistä todistusta, joka liittää sähköisen allekirjoituksen validointitiedot luonnolliseen henkilöön ja vahvistaa vähintään kyseisen henkilön nimen tai salanimen;”

d) korvataan 16 alakohta seuraavasti:

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

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

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

b) sähköisten allekirjoitusten tai sähköisten leimojen luominen;

c) sähköisten allekirjoitusten tai sähköisten leimojen validointi;

d) sähköisten allekirjoitusten, sähköisten leimojen, sähköisten allekirjoitusten varmenteiden tai sähköisten leimojen varmenteiden säilyttäminen;

e) hyväksyttyjen sähköisen allekirjoituksen etäluontivälineiden tai hyväksyttyjen sähköisen leiman etäluontivälineiden hallinnointi;

f) sähköisten attribuuttitodistusten myöntäminen;

fa) sähköisten attribuuttitodistusten validointi;

g) sähköisten aikaleimojen luominen;

ga) sähköisten aikaleimojen validointi;

gb) sähköisten rekisteröityjen jakelupalvelujen tarjoaminen;

gc) sähköisten rekisteröityjen jakelupalvelujen kautta toimitettujen tietojen ja niihin liittyvien todisteiden validointi;

h) sähköisten tietojen sähköinen arkistointi; tai

i) sähköisten tietojen tallentaminen sähköiseen tilikirjaan;”

da) korvataan 18 alakohta seuraavasti:

”18. ’vaatimustenmukaisuuden arviointilaitoksella’ asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa määriteltyä elintä, joka on akkreditoitu kyseisen asetuksen mukaisesti pätevästi arvioimaan hyväksyttyjen luottamuspalvelun tarjoajien ja niiden tarjoamien hyväksyttyjen luottamuspalvelujen vaatimustenmukaisuus tai sertifioimaan eurooppalainen digitaalisen identiteetin lompakko tai sähköisen tunnistamisen menetelmä;”

e) korvataan 21 alakohta seuraavasti:

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

f) lisätään 23 a ja 23 b alakohta seuraavasti:

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

23 b. ’hyväksytyllä sähköisen leiman etäluontivälineellä’ hyväksyttyä sähköisen leiman luontivälinettä, jota hyväksytty luottamuspalvelun tarjoaja hallinnoi leiman luojan puolesta 39 a artiklan mukaisesti;”

g) korvataan 29 alakohta seuraavasti:

”29. ’sähköisen leiman varmenteella’ sähköistä todistusta, joka liittää sähköisen leiman validointitiedot oikeushenkilöön ja vahvistaa kyseisen henkilön nimen;”

h) korvataan 41 alakohta seuraavasti:

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

i) lisätään 42 – 55 c alakohta seuraavasti:

”42. ’eurooppalaisella digitaalisen identiteetin lompakolla’ sähköisen tunnistamisen menetelmää, jonka avulla käyttäjä voi tallentaa ja hakea henkilöllisyyteensä liittyviä tietoja, mukaan lukien henkilön tunnistetiedot ja omaan henkilöllisyyteen liitetyt sähköiset attribuuttitodistukset, antaa niitä pyynnöstä luottaville osapuolille ja käyttää niitä todentamiseen verkossa ja tarvittaessa sen ulkopuolella 6 a artiklan mukaista palvelua varten; ja joka mahdollistaa hyväksytyillä sähköisillä allekirjoituksilla allekirjoittamisen ja hyväksyttyjen sähköisten leimojen käytön;

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;

45 a. ’virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämällä tai sen puolesta myönnetyllä 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 da artiklan mukaisesti ja jotka täyttävät liitteessä VII säädetyt vaatimukset;

46. ’virallisella lähteellä’ julkisen sektorin elimen tai yksityisen tahon vastuulla ylläpidettyä rekisteriä tai järjestelmää, joka sisältää ja tarjoaa luonnollisten tai oikeushenkilöiden attribuutteja ja jota pidetään näiden tietojen ensisijaisena lähteenä tai joka tunnustetaan todistusvoimaiseksi unionin tai kansallisen lainsäädännön mukaisesti, mukaan lukien hallintokäytännöt;

47. ’sähköisellä arkistoinnilla’ palvelua, jolla varmistetaan sähköisten tietojen vastaanotto, tallentaminen, hakeminen ja poistaminen, jotta voidaan taata niiden pysyvyys ja luettavuus sekä säilyttää niiden eheys ja luottamuksellisuus ja todistus alkuperästä koko säilytysajan;

48. ’hyväksytyllä sähköisellä arkistointipalvelulla’ sähköistä arkistointipalvelua, joka täyttää 45 ga artiklassa säädetyt vaatimukset;

49. ’EU:n digitaalisen identiteetin lompakon luotettavuusmerkillä’ todennettavissa olevaa yksinkertaista, tunnistettavaa ja selkeää osoitusta siitä, että eurooppalainen digitaalisen identiteetin lompakko on annettu käyttöön tämän asetuksen mukaisesti;

50. ’käyttäjän vahvalla todentamisella’ todentamista, jossa käytetään todentamistietojen luottamuksellisuuden suojaamiseksi menettelyä, joka perustuu vähintään kahteen toisistaan riippumattomaan todentamistekijään, jotka kuuluvat eri ryhmiin, jotka ovat tieto (jotain, minkä vain käyttäjä tietää), hallussapito (jotain, mitä vain käyttäjällä on hallussaan) ja erityinen ominaisuus (jotain, mitä käyttäjä on) siten, että yhden rikkominen ei aseta kyseenalaiseksi muiden luotettavuutta;

53. ’sähköisellä tilikirjalla’ sarjaa sähköisiä tietoja, joilla varmistetaan tietojen eheys ja kronologisen järjestyksen oikeellisuus;

53 a. ’hyväksytyllä sähköisellä tilikirjalla’ sähköistä tilikirjaa, joka täyttää 45 i artiklassa säädetyt vaatimukset;

54. ’henkilötiedoilla’ asetuksen (EU) 2016/679 4 artiklan 1 alakohdassa määriteltyjä tietoja;

55. ’tietueiden yhteensovittamisella’ prosessia, jossa henkilön tunnistetiedot, henkilön tunnistusmenetelmät, hyväksytyt sähköiset attribuuttitodistukset tai attribuuttitodistukset, jotka on myöntänyt virallisesta lähteestä vastaava julkisen sektorin elin tai jotka on myönnetty sen puolesta, yhdistetään tai liitetään samalle henkilölle kuuluvaan olemassa olevaan tiliin;

55 a. ’yksilöivällä ja pysyvällä tunnisteella’ tunnistetta, joka voi koostua joko yhdestä tai useammasta kansallisesta tai alakohtaisesta tunnisteesta, joka liittyy yksittäiseen käyttäjään tietyssä järjestelmässä ja joka on pysyvä ajallisesti;

55 b. ’tiedolla’ sähköisiä tietoja, jotka on tallennettu tietojen käsittelyä tukevien metatietojen (tai attribuuttien) kera;

55 c. ’eurooppalaisen digitaalisen identiteetin lompakon verkon ulkopuolisella käytöllä’ käyttäjän ja luottavan osapuolen välistä vuorovaikutusta fyysisessä paikassa, jolloin lompakkoa ei vaadita mahdollistamaan pääsyä etäjärjestelmiin sähköisten viestintäverkkojen kautta vuorovaikutusta varten.”

”*5 artikla*

Salanimien käyttö sähköisissä transaktioissa

Salanimien käyttöä sähköisissä transaktioissa ei kielletä, sanotun kuitenkaan rajoittamatta salanimille kansallisessa laissa annettavia oikeusvaikutuksia.”

5) Lisätään II jaksoon ennen 6 a artiklaa otsikko seuraavasti:

”I JAKSO

Eurooppalainen digitaalisen identiteetin lompakko;

7) Lisätään 6 a, 6 b, 6 c ja 6 d artikla seuraavasti:

”*6 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, kunkin jäsenvaltion on varmistettava, että eurooppalainen digitaalisen identiteetin lompakko annetaan käyttöön 24 kuukauden kuluessa 11 kohdassa ja 6 c artiklan 4 kohdassa tarkoitettujen täytäntöönpanosäädösten voimaantulosta.

2. Eurooppalainen digitaalisen identiteetin lompakko voidaan antaa käyttöön seuraavasti:

   a) sen antaa käyttöön jäsenvaltio;

   b) se annetaan käyttöön jäsenvaltion toimeksiannosta; tai

   c) se annetaan käyttöön jäsenvaltiosta itsenäisesti, mutta jäsenvaltio tunnustaa sen.

3. Eurooppalainen digitaalisen identiteetin lompakko on sähköisen tunnistamisen menetelmä, jonka avulla käyttäjän on voitava läpinäkyvällä ja käyttäjän jäljitettävissä olevalla tavalla

   a) pyytää, valita, yhdistää, tallentaa, poistaa ja esittää luottaville osapuolille sähköisiä attribuuttitodistuksia ja henkilön tunnistetietoja turvallisesti, myös todentamistarkoituksessa verkossa ja tarvittaessa verkon ulkopuolella julkisten ja yksityisten palvelujen käyttämiseksi, varmistaen samalla, että tietojen valikoiva luovuttaminen on mahdollista;

   b) allekirjoittaa hyväksytyillä sähköisillä allekirjoituksilla ja leimata käyttäen hyväksyttyjä sähköisiä leimoja.

4. Eurooppalaisten digitaalisen identiteetin lompakoiden on erityisesti

a) tarjottava yhteiset käyttöliittymät:

1) henkilön tunnistetietojen, hyväksyttyjen ja ei-hyväksyttyjen sähköisten attribuuttitodistusten tai hyväksyttyjen ja ei-hyväksyttyjen varmenteiden myöntämiseen eurooppalaiselle digitaalisen identiteetin lompakolle;

2) luottaville osapuolille, jotta ne voivat pyytää henkilön tunnistetietoja ja sähköisiä attribuuttitodistuksia;

3) henkilöiden tunnistetietojen tai sähköisten attribuuttitodistusten esittämiseksi luottaville osapuolille verkossa ja tarvittaessa myös verkon ulkopuolella;

4) jotta käyttäjä voi sallia vuorovaikutuksen eurooppalaisen digitaalisen identiteetin lompakon kanssa ja näyttää EU:n digitaalisen identiteetin lompakon luottamusmerkin;

b) oltava antamatta sähköisiä attribuuttitodistuksia myöntäville luottamuspalvelun tarjoajille mitään tietoja näiden attribuuttien käytöstä niiden myöntämisen jälkeen;

ba) varmistettava, että luottavien osapuolten henkilöllisyys voidaan validoida ottamalla käyttöön todentamismekanismeja 6 b artiklan mukaisesti;

c) täytettävä 8 artiklassa säädetyt korkeaa varmuustasoa koskevat vaatimukset, joita sovelletaan soveltuvin osin henkilöiden tunnistetietojen hallinnointiin ja käyttöön lompakon kautta, mukaan lukien sähköinen tunnistaminen ja todentaminen;

e) varmistettava, että 12 artiklan 4 kohdan d alakohdassa tarkoitetut henkilön tunnistetiedot edustavat yksilöivästi ja pysyvästi kyseistä lompakkoon liittyvää luonnollista henkilöä, oikeushenkilöä taikka luonnollista henkilöä tai oikeushenkilöä edustavaa luonnollista henkilöä.

4 a. Jäsenvaltioiden on säädettävä menettelyistä, joiden avulla käyttäjä voi ilmoittaa lompakkonsa mahdollisesta katoamisesta tai väärinkäytöstä ja pyytää sen peruuttamista.

5. Jäsenvaltioiden on luotava validointimekanismit eurooppalaisia digitaalisen identiteetin lompakoita varten, jotta voidaan

a) varmistaa, että lompakon aitous ja voimassaolo voidaan todentaa;

d) antaa käyttäjälle mahdollisuus todentaa luottavat osapuolet 6 b artiklan mukaisesti.

6. Eurooppalaiset digitaalisen identiteetin lompakot on annettava käyttöön osana ilmoitettua sähköisen tunnistamisen järjestelmää, jonka varmuustaso on korkea.

6 a. Eurooppalaisten digitaalisen identiteetin lompakoiden käyttöön antamisen, käytön todentamistarkoituksessa ja peruuttamisen on oltava maksutonta luonnollisille henkilöille.

6 b. Jäsenvaltiot voivat kansallisen lainsäädännön mukaisesti säätää eurooppalaisten digitaalisen identiteetin lompakoiden lisätoiminnoista, mukaan lukien yhteentoimivuus olemassa olevien kansallisten sähköisen tunnistamisen menetelmien kanssa, sanotun kuitenkaan rajoittamatta 6 db artiklan soveltamista.

7. Oman eurooppalaisen digitaalisen identiteetin lompakon ja sen sisältämien tietojen on oltava täysin käyttäjän hallinnassa. Eurooppalaisen digitaalisen identiteetin lompakon käyttöön antaja ei saa kerätä lompakon käytöstä tietoja, jotka eivät ole välttämättömiä lompakkopalvelujen tarjoamiseksi, eikä yhdistää henkilön tunnistetietoja eikä muita henkilötietoja, jotka on tallennettu tai jotka liittyvät eurooppalaisen digitaalisen identiteetin lompakon käyttöön, muihin kyseisen käyttöön antajan tai kolmansien osapuolten tarjoamista palveluista saatuihin henkilötietoihin, jotka eivät ole välttämättömiä lompakkopalvelujen tarjoamiseksi, paitsi jos käyttäjä on sitä nimenomaisesti pyytänyt. Eurooppalaisten digitaalisen identiteetin lompakoiden tarjoamiseen liittyvät henkilötiedot on pidettävä loogisesti erillään kaikista muista tiedoista, joita eurooppalaisen identiteetin lompakon käyttöön antajan hallussa on. Jos eurooppalaisen digitaalisen identiteetin lompakon tarjoavat yksityiset osapuolet 2 kohdan b ja c alakohdan mukaisesti, sovelletaan 45 f artiklan 4 kohdan säännöksiä soveltuvin osin.

7 a. Jäsenvaltioiden on ilmoitettava komissiolle ilman aiheetonta viivytystä tiedot seuraavista:

a) elin, joka vastaa eurooppalaisia digitaalisen identiteetin lompakoita käyttävien ilmoitettujen luottavien osapuolten luettelon laatimisesta ja ylläpitämisestä 6 b artiklan 2 kohdan mukaisesti;

b) elimet, jotka vastaavat eurooppalaisten digitaalisen identiteetin lompakoiden tarjoamisesta 6 a artiklan 1 kohdan mukaisesti;

c) elimet, jotka ovat vastuussa sen varmistamisesta, että henkilön tunnistetiedot liitetään lompakkoon 6 a artiklan 4 kohdan e alakohdan mukaisesti.

Ilmoituksessa on myös annettava tiedot mekanismista, joka mahdollistaa 12 artiklan 4 kohdassa tarkoitettujen henkilöiden tunnistetietojen ja luottavien osapuolten henkilöllisyyden validoinnin.

Komissio asettaa julkisesti saataville suojatusti tässä kohdassa tarkoitetut tiedot sähköisesti allekirjoitetussa tai leimatussa muodossa, joka soveltuu automaattiseen käsittelyyn.

8. Tämän asetuksen 11 artiklaa sovelletaan soveltuvien osin eurooppalaiseen digitaalisen identiteetin lompakkoon.

9. Tämän asetuksen 24 artiklan 2 kohdan b, e, g ja h alakohtaa sovelletaan soveltuvin osin eurooppalaisia digitaalisen identiteetin lompakoita käyttöön antaviin tahoihin.

10. Eurooppalaisen digitaalisen identiteetin lompakon on oltava esteettömästi vammaisten henkilöiden saatavilla direktiivissä 2019/882 vahvistettujen esteettömyysvaatimusten mukaisesti.

11. Komissio vahvistaa kuuden kuukauden kuluessa tämän asetuksen voimaantulosta tekniset ja toiminnalliset eritelmät ja viitestandardit 3, 4, 5 ja 7 a kohdassa tarkoitettuja vaatimuksia varten antamalla eurooppalaisen digitaalisen identiteetin lompakon toteuttamista koskevan täytäntöönpanosäädöksen. Tämä täytäntöönpanosäädös hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

11 a. Komissio vahvistaa tekniset ja toiminnalliset eritelmät sekä viitestandardit, joilla helpotetaan eurooppalaisen digitaalisen identiteetin lompakon käyttäjien asiakassuhteen perustamista käyttäen joko korkean varmuustason mukaista sähköisen tunnistamisen menetelmää tai korotetun varmuustason mukaista sähköisen tunnistamisen menetelmää yhdessä sellaisten täydentävien asiakassuhteen perustamisen etämenettelyjen kanssa, jotka yhdessä täyttävät korkean varmuustason vaatimukset. Tämä täytäntöönpanosäädös hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

6 b artikla

Eurooppalaisten digitaalisen identiteetin lompakoiden luottavat osapuolet

1. Jos yksityisiä tai julkisia palveluja tarjoavat luottavat osapuolet aikovat luottaa tämän asetuksen mukaisesti tarjottuihin eurooppalaisiin digitaalisen identiteetin lompakoihin, niiden on ilmoitettava siitä sille jäsenvaltiolle, johon luottavat osapuolet ovat sijoittautuneet.

1 a. Ilmoitusmenettelyn on oltava kustannustehokas ja oikeassa suhteessa riskiin, ja sillä on varmistettava, että luottavat osapuolet toimittavat vähintään tiedot, joita tarvitaan todentautumiseksi eurooppalaisiin digitaalisen identiteetin lompakoihin. Tähän olisi sisällyttävä vähintään jäsenvaltio, johon ne ovat sijoittautuneet, sekä luottavan osapuolen nimi ja tarvittaessa sen rekisterinumero virallisissa rekistereissä olevassa muodossa.

1 b. Ilmoitusvaatimus ei vaikuta muihin unionin tai kansallisen lainsäädännön mukaisiin ilmoitus- ja rekisteröintivaatimuksiin, kuten erityisiin henkilötietoryhmiin sovellettaviin vaatimuksiin, jotka saattavat edellyttää erillisiä lupavaatimuksia.

1 c. Jäsenvaltiot voivat vapauttaa luottavat osapuolet ilmoitusvaatimuksesta, jos unionin tai kansallisessa lainsäädännössä ei säädetä erityisistä ilmoitus- tai rekisteröintivaatimuksista eurooppalaisen digitaalisen identiteetin lompakon kautta toimitettujen tietojen saamiseksi. Poikkeuksen saaneiden luottavien osapuolten ei välttämättä tarvitse todentautua eurooppalaisiin digitaalisen identiteetin lompakoihin.

1 d. Luottavien osapuolten, joille on annettu ilmoitus tämän artiklan mukaisesti, on ilmoitettava viipymättä jäsenvaltiolle mahdollisista myöhemmistä muutoksista alun perin annettuihin tietoihin.

2. Luottavien osapuolten on varmistettava 6 a artiklan 4 kohdan ba alakohdassa tarkoitettujen todentamismekanismien täytäntöönpano.

3. Luottavat osapuolet vastaavat eurooppalaisista digitaalisen identiteetin lompakoista peräisin olevien 6 a artiklan 4 kohdan a alakohdan 2 alakohdassa tarkoitetun yhteisen käyttöliittymän kautta saatujen henkilöllisyyksien ja sähköisten attribuuttitodistusten todentamismenettelyn toteuttamisesta.

4. Komissio vahvistaa kuuden kuukauden kuluessa tämän asetuksen voimaantulosta tekniset ja toiminnalliset eritelmät 1, 1 a ja 1 d kohdassa tarkoitettuja vaatimuksia varten antamalla 6 a artiklan 11 kohdassa tarkoitetun eurooppalaisen digitaalisen identiteetin lompakon toteuttamista koskevan täytäntöönpanosäädöksen. Tämä täytäntöönpanosäädös hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

6 c artikla

Eurooppalaisten digitaalisen identiteetin lompakoiden sertifiointi

1. Kyberturvallisuusasetuksen 60 artiklan ja 4 kohdan a, aa ja aaa alakohdassa tarkoitettujen järjestelmien, eritelmien, standardien ja menetelmien mukaisesti akkreditoidut sekä jäsenvaltioiden nimeämät vaatimustenmukaisuuden arviointilaitokset sertifioivat sen, että eurooppalaiset digitaalisen identiteetin lompakot noudattavat 6 a artiklan 3, 4 ja 5 kohdassa säädettyjä vaatimuksia, 6 a artiklan 7 kohdassa säädettyä loogista erillään pitoa koskevaa vaatimusta ja tarvittaessa 6 a artiklan 11 a kohdassa säädettyjä vaatimuksia. Sertifiointi saa kestää enintään viisi vuotta, ja sen edellytyksenä on säännöllinen kahden vuoden välein tehtävä haavoittuvuusarviointi. Jos haavoittuvuuksia havaitaan eikä niitä korjata kolmen kuukauden kuluessa, sertifiointi peruutetaan.

2. Edellä olevan 6 a artiklan 7 kohdan mukaisten tietosuojavaatimusten noudattamisen osalta 1 kohdan mukaista sertifiointia voidaan täydentää asetuksen (EU) 2016/679 42 artiklan mukaisella sertifioinnilla.

3. Edellä 1 kohdassa tarkoitetut vaatimustenmukaisuuden arviointilaitokset sertifioivat sen, että eurooppalaiset digitaalisen identiteetin lompakot tai niiden osat ovat 6 a artiklan 3, 4, 5 ja 7 kohdassa ja tapauksen mukaan 11 a artiklassa vahvistettujen kyberturvallisuuden kannalta merkityksellisten vaatimusten mukaisia asetuksen (EU) 2019/881 mukaisten asiaankuuluvien kyberturvallisuuden sertifiointijärjestelmien puitteissa, sellaisina kuin niihin viitataan 4 a ja 4 aa kohdan mukaisesti.

3 a. Sertifioituihin eurooppalaisiin digitaalisen identiteetin lompakoihin ei sovelleta 7 ja 9 artiklassa tarkoitettuja vaatimuksia.

4. Komissio vahvistaa 6 kuukauden kuluessa tämän asetuksen voimaantulosta täytäntöönpanosäädöksillä seuraavat:

a) luettelo asetuksen (EU) 2019/881 mukaisista kyberturvallisuuden sertifiointijärjestelmistä, joita tarvitaan 3 kohdassa tarkoitettua eurooppalaisten digitaalisen identiteetin lompakoiden sertifiointia varten;

aa) eritelmät, menettelyt ja viitestandardit, jotka koskevat niiden käyttöä a alakohdan mukaisesti luetteloiduissa asiaankuuluvissa kyberturvallisuuden sertifiointijärjestelmissä;

aaa) luettelo määritelmistä, menettelyistä ja viitestandardeista, joissa vahvistetaan yhteiset sertifiointia koskevat vaatimukset, joita ei kateta asetuksen (EU) 2019/881 mukaisissa asiaankuuluvissa kyberturvallisuuden sertifiointijärjestelmissä, 1 kohdassa tarkoitettua sertifiointia varten ja joiden tarkoituksena on osoittaa, että eurooppalainen digitaalisen identiteetin lompakko täyttää 1 kohdassa tarkoitetut vaatimukset;

b) tekniset, menettelylliset, organisatoriset ja toiminnalliset eritelmät, jotka koskevat 1 kohdassa tarkoitettujen vaatimustenmukaisuuden arviointilaitosten nimeämistä ja aaa alakohdan mukaisesti vahvistettujen sertifiointia koskevien vaatimusten osalta näiden laitosten käyttämien sertifiointijärjestelmien ja niihin liittyvien arviointimenetelmien sekä niiden myöntämien sertifikaattien ja sertifiointiraporttien seurantaa ja uudelleentarkastelua.

5. Jäsenvaltioiden on ilmoitettava komissiolle 1 kohdassa tarkoitettujen julkisten tai yksityisten elinten nimet ja osoitteet. Komissio asettaa nämä tiedot jäsenvaltioiden saataville.

6. Edellä 4 kohdassa tarkoitetut täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

6 d artikla

Sertifioitujen eurooppalaisten digitaalisen identiteetin lompakoiden luettelon julkaiseminen

1. Jäsenvaltioiden on ilman aiheetonta viivytystä ilmoitettava komissiolle eurooppalaisista digitaalisen identiteetin lompakoista, jotka on annettu käyttöön 6 a artiklan mukaisesti ja jotka 6 c artiklan 1 kohdassa tarkoitetut elimet ovat sertifioineet. Niiden on ilman aiheetonta viivytystä ilmoitettava komissiolle, jos sertifiointi peruutetaan.

2. Saamiensa tietojen perusteella komissio laatii ja julkaisee koneellisesti luettavassa muodossa olevan luettelon sertifioiduista eurooppalaisista digitaalisen identiteetin lompakoista sekä pitää sitä ajan tasalla.

3. Komissio määrittelee kuuden kuukauden kuluessa tämän asetuksen voimaantulosta 1 ja 2 kohdan soveltamiseen liittyvät muotoseikat ja menettelyt antamalla 6 a artiklan 11 kohdassa tarkoitetun eurooppalaisen digitaalisen identiteetin lompakon toteuttamista koskevan täytäntöönpanosäädöksen. Tämä täytäntöönpanosäädös hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

6 da artikla

Eurooppalaisten digitaalisen identiteetin lompakoiden tietoturvaloukkaus

1. Jos 6 a artiklan mukaisesti tarjottuihin eurooppalaisiin digitaalisen identiteetin lompakoihin tai 6 a artiklan 5 kohdan a, d tai e alakohdassa tarkoitettuun validointimekanismiin kohdistuu tietoturvaloukkaus tai niiden turvallisuus on osittain vaarantunut tavalla, joka vaikuttaa niiden luotettavuuteen tai muiden eurooppalaisten digitaalisen identiteetin lompakoiden luotettavuuteen, kyseessä olevien lompakoiden käyttöön antajan on ilman aiheetonta viivytystä keskeytettävä eurooppalaisen digitaalisen identiteetin lompakon käyttöön antaminen ja sen käyttö. Jäsenvaltion, jossa kyseessä olevia lompakoita on tarjottu, on ilmoitettava asiasta jäsenvaltioille ja komissiolle ilman aiheetonta viivytystä. Asianomaisten lompakoiden käyttöön antajan tai jäsenvaltion on ilmoitettava asiasta luottaville osapuolille ja käyttäjille.

2. Kun 1 kohdassa tarkoitettu loukkaus tai turvallisuuden vaarantuminen on korjattu, lompakon käyttöön antajan on aloitettava uudelleen eurooppalaisen digitaalisen identiteetin lompakon käyttöön antaminen ja käyttö. Jäsenvaltion, jossa kyseessä olevia lompakoita on tarjottu, on ilmoitettava asiasta jäsenvaltioille ja komissiolle ilman aiheetonta viivytystä. Asianomaisten lompakoiden käyttöön antajan tai jäsenvaltion on ilmoitettava asiasta ilman aiheetonta viivytystä luottaville osapuolille ja käyttäjille.

3. Jos 1 kohdassa tarkoitettua loukkausta tai vaarantumista ei ole korjattu kolmen kuukauden kuluessa keskeyttämisestä, asianomaisen jäsenvaltion on poistettava eurooppalainen digitaalisen identiteetin lompakko käytöstä ja ilmoitettava asiasta muille jäsenvaltioille ja komissiolle. Jos se on rikkomisen vakavuuden vuoksi perusteltua, eurooppalainen digitaalisen identiteetin lompakko on poistettava käytöstä ilman aiheetonta viivytystä.

4. Komissio julkaisee Euroopan unionin virallisessa lehdessä vastaavat tarkistukset 6 d artiklassa tarkoitettuun luetteloon ilman aiheetonta viivytystä.

5. Komissio määrittelee kuuden kuukauden kuluessa tämän asetuksen voimaantulosta tarkemmin 1, 2 ja 3 kohdassa tarkoitetut toimenpiteet antamalla 6 a artiklan 11 kohdassa tarkoitetun eurooppalaisen digitaalisen identiteetin lompakon toteuttamista koskevan täytäntöönpanosäädöksen. Tämä täytäntöönpanosäädös hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

6 db artikla

Eurooppalaisten digitaalisen identiteetin lompakoiden rajatylittävä käyttö

1. Kun jäsenvaltio edellyttää sähköisen tunnistamisen menetelmän ja todentamisen avulla tehtävää sähköistä tunnistamista julkisen sektorin elimen tarjoaman verkkopalvelun käyttämiseksi, niiden on hyväksyttävä myös tämän asetuksen mukaisesti tarjotut eurooppalaiset digitaalisen identiteetin lompakot käyttäjän todentamista varten.

2. Jos kansallisessa tai unionin lainsäädännössä edellytetään, että palveluja tarjoavat yksityiset luottavat osapuolet, lukuun ottamatta komission suosituksessa 2003/361/EY 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, yksityisten luottavien osapuolten on viimeistään 12 kuukauden kuluttua eurooppalaisten digitaalisen identiteetin lompakoiden tarjoamisesta 6 a artiklan 1 kohdan mukaisesti ja ainoastaan käyttäjän vapaaehtoisesta pyynnöstä hyväksyttävä myös tämän artiklan mukaisesti tarjottujen eurooppalaisten digitaalisen identiteetin lompakoiden käyttö sen verkkopalvelun vähimmäistietojen osalta, jota varten käyttäjän todentamista pyydetään.

3. Jos asetuksen [digipalvelusäädöksen viite] 25 artiklan 1 kohdassa määritellyt erittäin suuret verkkoalustat 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.

4. Komissio yhdessä jäsenvaltioiden kanssa kannustaa ja helpottaa käytännesääntöjen kehittämistä, jotta voidaan edistää eurooppalaisten digitaalisen identiteetin lompakoiden laajaa saatavuutta ja käytettävyyttä tämän asetuksen soveltamisalalla. Käytännesäännöillä on edistettävä sitä, että erityisesti palveluntarjoajat, jotka käyttävät kolmannen osapuolen tarjoamia sähköisiä tunnistuspalveluja käyttäjien todentamisessa, hyväksyvät tämän asetuksen soveltamisalalla sähköisen tunnistamisen menetelmät, myös eurooppalaiset digitaalisen identiteetin lompakot. Komissio helpottaa tällaisten käytännesääntöjen laatimista tiiviissä yhteistyössä kaikkien asiaankuuluvien sidosryhmien kanssa ja kannustaa palveluntarjoajia saattamaan käytännesääntöjen laatimisen päätökseen 12 kuukauden kuluessa tämän asetuksen hyväksymisestä ja panemaan ne tehokkaasti täytäntöön 18 kuukauden kuluessa asetuksen hyväksymisestä.

5. Komissio arvioi 24 kuukauden kuluessa eurooppalaisten digitaalisen identiteetin lompakoiden käyttöönotosta, annetaanko eurooppalaisten digitaalisen identiteetin lompakoiden kysyntää, saatavuutta ja käytettävyyttä koskevan näytön perusteella muille yksityisille verkkopalvelujen tarjoajille velvoite hyväksyä eurooppalaisten digitaalisen identiteetin lompakoiden käyttö ainoastaan käyttäjän vapaaehtoisesta pyynnöstä. Arviointiperusteita ovat muun muassa käyttäjäkunnan laajuus, palveluntarjoajien rajatylittävä läsnäolo, teknologian kehitys, käyttötapojen kehittyminen ja kuluttajakysyntä.

8) Lisätään ennen 7 artiklaa otsikko seuraavasti:

”II JAKSO

SÄHKÖISEN TUNNISTAMISEN JÄRJESTELMÄT”

9) Korvataan 7 artiklan johdantokappale seuraavasti:

”Jäsenvaltioiden, jotka eivät ole vielä tehneet niin 9 artiklan 1 kohdan mukaisesti, on ilmoitettava 24 kuukauden kuluessa 6 a artiklan 11 kohdassa ja 6 c artiklan 4 kohdassa tarkoitettujen täytäntöönpanosäädösten voimaantulosta vähintään yksi sähköisen tunnistamisen järjestelmä, johon sisältyy vähintään yksi korkean varmuustason tunnistamisen menetelmä. Sähköisen tunnistamisen järjestelmä voidaan ilmoittaa 9 artiklan 1 kohdan mukaisesti, edellyttäen että kaikki seuraavat ehdot täyttyvät:”

10) Korvataan 9 artiklan 2 ja 3 kohta seuraavasti:

”2. Komissio julkaisee Euroopan unionin virallisessa lehdessä luettelon tämän artiklan 1 kohdan nojalla ilmoitetuista sähköisen tunnistamisen järjestelmistä sekä niitä koskevat perustiedot.

3. Komissio julkaisee Euroopan unionin virallisessa lehdessä muutokset 2 kohdassa tarkoitettuun luetteloon kuukauden kuluessa muutosilmoituksen vastaanottamisesta.”

12) Lisätään 11 a artikla seuraavasti:

”*11 a artikla*

Tietueiden yhteensovittaminen

1. Jos todentamiseen käytetään ilmoitettuja sähköisen tunnistamisen menetelmiä tai eurooppalaisia digitaalisen identiteetin lompakoita, luottavina osapuolina toimivien jäsenvaltioiden on varmistettava tietueiden yhteensovittaminen.

2. Jäsenvaltioiden on eurooppalaisten digitaalisen identiteetin lompakoiden tarjoamiseksi sisällytettävä 12 artiklan 4 kohdan d alakohdassa tarkoitettuihin henkilöiden vähimmäistunnistetietoihin vähintään yksi unionin ja kansallisen lainsäädännön mukainen yksilöivä ja pysyvä tunniste, jotta käyttäjä voidaan tämän omasta pyynnöstä tunnistaa tapauksissa, joissa lainsäädännössä edellytetään käyttäjän tunnistamista.

2 a. Jäsenvaltioiden on säädettävä teknisistä ja organisatorisista toimenpiteistä, joilla varmistetaan tietueiden yhteensovittamiseen käytettävien henkilötietojen korkeatasoinen suoja ja estetään käyttäjien profilointi.

2 aa. Jäsenvaltiot voivat säätää kansallisen lainsäädännön mukaisesti, että eurooppalaisen digitaalisen identiteetin lompakon käyttäjän on voitava pyytää, että yksilöivä ja pysyvä tunniste, joka sisältyy henkilön vähimmäistunnistetietoihin ja on liitetty lompakkoon 6 a artiklan 4 kohdan e alakohdan mukaisesti, korvataan toisella jäsenvaltion antamalla yksilöivällä ja pysyvällä tunnisteella.

3. Komissio määrittelee kuuden kuukauden kuluessa tämän asetuksen voimaantulosta tarkemmin 1 kohdassa tarkoitetut toimenpiteet antamalla täytäntöönpanosäädöksen. Tämä täytäntöönpanosäädös hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

3 a. Komissio määrittelee kuuden kuukauden kuluessa tämän asetuksen voimaantulosta tarkemmin 2 ja 2 aa kohdassa tarkoitetut toimenpiteet antamalla täytäntöönpanosäädöksen. Tämä täytäntöönpanosäädös hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

13) Muutetaan 12 artikla seuraavasti:

"Yhteistyö ja yhteentoimivuus"

a) kumotaan 3 kohdan d alakohta;

b) korvataan 4 kohdan d alakohta seuraavasti:

”d) viittauksesta henkilön tunnistetietojen vähimmäismäärään, joka tarvitaan luonnollisen henkilön, oikeushenkilön taikka luonnollista tai oikeushenkilöä edustavan luonnollisen henkilön yksilöivään ja pysyvään tunnistamiseen;”

ba) lisätään 5 kohtaan c alakohta seuraavasti:

”(c) samanlainen lähestymistapa verkkopalveluihin, jotka hyväksyvät tämän asetuksen mukaisesti tarjottavien eurooppalaisten digitaalisen identiteetin lompakoiden käytön;”

c) korvataan 6 kohdan a alakohta seuraavasti:

”a) sähköisen tunnistamisen järjestelmiä ja erityisesti yhteentoimivuuteen, tietueiden yhteensovittamiseen ja varmuustasoihin liittyviä teknisiä vaatimuksia koskevien tietojen, kokemusten ja hyvien käytäntöjen vaihto;”

ca) lisätään 6 kohtaan e alakohta seuraavasti:

”e) tietojen, kokemusten ja hyvien käytäntöjen vaihto sekä suuntaviivojen antaminen siitä, miten verkkopalveluja voidaan suunnitella, kehittää ja toteuttaa eurooppalaisten digitaalisen identiteetin lompakoiden käyttöä varten”.

14) Lisätään 12 a ja 12 b artikla seuraavasti:

”*12 a artikla*

Sähköisen tunnistamisen järjestelmien sertifiointi

1. Ilmoitettavien sähköisen tunnistamisen järjestelmien vaatimustenmukaisuus tässä asetuksessa säädettyjen vaatimusten kanssa on sertifioitava sen osoittamiseksi, että tällaiset järjestelmät tai niiden osat täyttävät 8 artiklan 2 kohdassa säädetyt vaatimukset, jotka koskevat asetuksen (EU) 2019/881 mukaisen asiaankuuluvan kyberturvallisuuden sertifiointijärjestelmän tai sen osien mukaisten sähköisen tunnistamisen järjestelmien varmuustasoja, siltä osin kuin kyberturvallisuussertifikaatti tai sen osat kattavat 8 artiklan 2 kohdassa säädetyt sähköisen tunnistamisen järjestelmien varmuustasoja koskevat vaatimukset. Sertifiointi saa kestää enintään viisi vuotta, ja sen edellytyksenä on säännöllinen kahden vuoden välein tehtävä haavoittuvuusarviointi. Jos haavoittuvuuksia havaitaan eikä niitä korjata kolmen kuukauden kuluessa, sertifiointi peruutetaan.

   Sertifioinnin suorittavat jäsenvaltioiden nimeämät akkreditoidut julkiset tai yksityiset vaatimustenmukaisuuden arviointilaitokset asetuksen (EY) N:o 765/2008 mukaisesti.

2. 12 artiklan 6 kohdan c alakohdassa tarkoitettua sähköisen tunnistamisen järjestelmien vertaisarviointia ei sovelleta 1 kohdan mukaisesti sertifioituihin sähköisen tunnistamisen järjestelmiin tai niiden osiin.

2 a. Sen estämättä, mitä tämän artiklan 2 kohdassa säädetään, jäsenvaltiot voivat pyytää ilmoituksen tehneeltä jäsenvaltiolta lisätietoja sähköisen tunnistamisen järjestelmistä tai niiden osista, jotka on sertifioitu tämän artiklan 2 kohdan mukaisesti.

3. Jäsenvaltioiden on ilmoitettava komissiolle 1 kohdassa tarkoitetun julkisen tai yksityisen tahon nimi ja osoite. Komissio asettaa nämä tiedot jäsenvaltioiden saataville.

12 b artikla

Pääsy laitteisto- ja ohjelmisto-ominaisuuksiin

Eurooppalaisten digitaalisen identiteetin lompakoiden käyttöön antajat ja ilmoitettujen sähköisen tunnistamisen menetelmien myöntäjät, jotka toimivat kaupallisessa tai ammatillisessa ominaisuudessa ja käyttävät 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 asetuksen (EU) 2022/1925 2 artiklan 21 kohdan mukaisia yrityskäyttäjiä.”

17) Korvataan 13 artiklan 1 kohta seuraavasti:

”1. Sen estämättä, mitä tämän artiklan 2 kohdassa säädetään, luottamuspalvelun tarjoajat ovat vastuussa luonnolliselle henkilölle tai oikeushenkilölle tahallaan tai tuottamuksesta aiheutetusta vahingosta, joka johtuu tämän asetuksen mukaisten velvoitteiden noudattamatta jättämisestä.

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

Hyväksytyn luottamuspalvelun tarjoajan oletetaan toimineen tahallaan tai tuottamuksesta, ellei kyseinen hyväksytty luottamuspalvelun tarjoaja todista, että ensimmäisessä alakohdassa tarkoitettu vahinko on tapahtunut ilman kyseisen hyväksytyn luottamuspalvelun tarjoajan tahallisuutta tai tuottamuksellisuutta.”

18) Korvataan 14 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 hyväksyttyjen luottamuspalvelun tarjoajien tarjoamat hyväksytyt luottamuspalvelut, jos kolmannesta maasta tai kansainvälisestä järjestöstä lähtöisin olevat luottamuspalvelut tunnustetaan unionin ja kolmannen maan tai kansainvälisen järjestön välillä täytäntöönpanopäätöksen tai Euroopan unionin toiminnasta 218 artiklan mukaisesti tehdyn sopimuksen nojalla.

2. Edellä 1 kohdassa tarkoitetuilla täytäntöönpanopäätöksillä ja sopimuksilla on varmistettava, että kolmannessa maassa tai kansainvälisessä järjestössä toimivat luottamuspalvelun tarjoajat ja niiden tarjoamat luottamuspalvelut täyttävät unionin alueelle sijoittautuneisiin hyväksyttyihin luottamuspalvelun tarjoajiin ja niiden tarjoamiin hyväksyttyihin luottamuspalveluihin sovellettavat vaatimukset. Kolmansien maiden ja kansainvälisten järjestöjen on erityisesti laadittava ja julkaistava luotettava luettelo tunnustetuista luottamuspalvelun tarjoajista ja ylläpidettävä sitä.

   Edellä 1 kohdassa tarkoitetuilla sopimuksilla on varmistettava, että unionin alueelle sijoittautuneiden hyväksyttyjen luottamuspalvelun tarjoajien tarjoamat hyväksytyt luottamuspalvelut tunnustetaan oikeusvaikutuksiltaan vastaaviksi kuin kolmannessa maassa tai kansainvälisessä järjestössä, jonka kanssa sopimus on tehty, toimivien luottamuspalvelun tarjoajien luottamuspalvelut.

3. Edellä 1 kohdassa tarkoitetut täytäntöönpanopäätökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

19) Korvataan 15 artikla seuraavasti:

”15 artikla

Esteettömyys vammaisten henkilöiden näkökulmasta

Luottamuspalvelujen tarjoaminen ja niiden tarjoamisessa käytetyt loppukäyttäjätuotteet on tehtävä vammaisille henkilöille esteettömiksi tuotteiden ja palvelujen esteettömyysvaatimuksista annetussa direktiivissä 2019/882 vahvistettujen esteettömyysvaatimusten mukaisesti.”

20) Muutetaan 17 artikla seuraavasti:

a) muutetaan 4 kohta seuraavasti:

1) korvataan 4 kohdan c alakohta seuraavasti:

”c) direktiivin (EU) XXXX/XXXX [NIS2-direktiivi] nojalla nimetyille asianomaisten jäsenvaltioiden asiaankuuluville kansallisille toimivaltaisille viranomaisille tiedottaminen kaikista merkittävistä tietoturvaloukkauksista tai eheyden menetyksistä, jotka ne ovat saaneet tietoonsa suorittaessaan tehtäviään. Jos merkittävä tietoturvaloukkaus tai eheyden menetys koskee muita jäsenvaltioita, valvontaelimen on ilmoitettava asiasta direktiivin (EU) XXXX/XXXX (NIS2-direktiivi) mukaisesti nimetylle asianomaisen jäsenvaltion keskitetylle yhteyspisteelle ja tämän asetuksen 17 artiklan mukaisesti nimetyille valvontaelimille muissa asianomaisissa jäsenvaltioissa. Ilmoituksen vastaanottaneen valvontaelimen on tiedotettava asiasta yleisölle tai vaadittava luottamuspalvelun tarjoajaa tiedottamaan siitä, jos se katsoo, että tietoturvaloukkauksen tai eheyden menetyksen julkistaminen on yleisen edun mukaista.”

2) Korvataan f alakohta seuraavasti:

”f) yhteistyön tekeminen asetuksen (EU) 2016/679 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.”

b) korvataan 6 kohta seuraavasti:

”6. Kunkin valvontaelimen on toimitettava komissiolle joka vuosi viimeistään 31 päivänä maaliskuuta kertomus tärkeimmistä toimistaan edellisenä kalenterivuonna.”

c) korvataan 8 kohta seuraavasti:

”8. Komissio hyväksyy 12 kuukauden kuluessa tämän asetuksen voimaantulosta ohjeet siitä, miten valvontaelimet hoitavat 4 kohdassa tarkoitettuja tehtäviä, ja määrittelee 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen annettavilla täytäntöönpanosäädöksillä 6 kohdassa tarkoitetun kertomuksen muodot ja menettelyt.”

21) Muutetaan 18 artikla seuraavasti:

a) korvataan 18 artiklan otsikko seuraavasti:

”Keskinäinen avunanto ja yhteistyö”

b) korvataan 1 kohta seuraavasti:

”1. Valvontaelinten on tehtävä yhteistyötä luottamuspalvelujen tarjoamista koskevien hyvien käytäntöjen ja tietojen vaihtamiseksi.”

c) lisätään 4 ja 5 kohta seuraavasti:

”4. Euroopan parlamentin ja neuvoston direktiivin (EU) XXXX/XXXX [NIS2-direktiivi] mukaisten valvontaelinten ja kansallisten toimivaltaisten viranomaisten on tehtävä yhteistyötä ja avustettava toisiaan sen varmistamiseksi, että luottamuspalvelun tarjoajat noudattavat tässä asetuksessa ja direktiivissä (EU) XXXX/XXXX [NIS2-direktiivi] säädettyjä vaatimuksia. Valvontaelinten on pyydettävä direktiivin XXXX/XXXX [NIS2-direktiivi] mukaisia kansallisia toimivaltaisia viranomaisia toteuttamaan valvontatoimia sen varmistamiseksi, että luottamuspalvelun tarjoajat noudattavat direktiivin XXXX/XXXX [NIS2-direktiivi] vaatimuksia, vaatimaan luottamuspalvelun tarjoajia korjaamaan näiden vaatimusten noudattamatta jättäminen, toimittamaan viipymättä luottamuspalvelun tarjoajiin liittyvien valvontatoimien tulokset ja tiedottamaan valvontaelimille direktiivin XXXX/XXXX [NIS2-direktiivi] mukaisesti ilmoitetuista merkityksellisistä poikkeamista.

5. Komissio vahvistaa 12 kuukauden kuluessa tämän asetuksen voimaantulosta tarvittavat menettelytavat 1 kohdassa tarkoitetun valvontaviranomaisten välisen yhteistyön helpottamiseksi antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

21 a) Lisätään 19 a artikla seuraavasti:

”Ei-hyväksyttyjä luottamuspalvelun tarjoajia koskevat vaatimukset”

1. Ei-hyväksyttyjä luottamuspalveluja tarjoavan ei-hyväksytyn luottamuspalvelun tarjoajan on

a) noudatettava asianmukaisia toimintaperiaatteita ja toteutettava vastaavat toimenpiteet ei-hyväksyttyjen luottamuspalvelujen tarjoamiseen kohdistuvien oikeudellisten, liiketoiminnallisten, operatiivisten ja muiden suorien tai välillisten riskien hallitsemiseksi. Sen estämättä, mitä direktiivin XXXX/XXX [NIS2-direktiivi] 18 artiklassa säädetään, näihin toimenpiteisiin on sisällyttävä vähintään seuraavat:

i) palveluun rekisteröitymiseen ja asiakassuhteen perustamismenettelyihin liittyvät toimenpiteet;

ii) menettelyllisiin tai hallinnollisiin tarkastuksiin liittyvät toimenpiteet;

iii) palvelujen hallinnointiin ja toteuttamiseen liittyvät toimenpiteet;

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

2. Komissio täsmentää 12 kuukauden kuluessa tämän asetuksen voimaantulosta 1 a kohdassa tarkoitettuihin toimenpiteisiin liittyvät tekniset ominaisuudet antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

22) 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) XXXX/XXXX [NIS2-direktiivi] 18 artiklassa säädetyt vaatimukset. Hyväksyttyjen luottamuspalvelun tarjoajien on toimitettava tarkastuksen perusteella laadittava vaatimustenmukaisuuden arviointikertomus valvontaelimelle kolmen työpäivän kuluessa sen vastaanottamisesta.”

aa) lisätään kohta seuraavasti:

”1 a. Jäsenvaltiot voivat säätää, että hyväksyttyjen luottamuspalvelun tarjoajien on ilmoitettava etukäteen valvontaelimelle suunnitelluista tarkastuksista ja sallittava pyynnöstä valvontaelimen osallistuminen tarkkailijana.”

b) korvataan 2 kohdan viimeinen virke seuraavasti:

”Jos näyttää siltä, että henkilötietojen suojaan liittyviä sääntöjä on rikottu, valvontaelimen on ilman aiheetonta viivytystä ilmoitettava siitä asetuksen (EU) 2016/679 mukaisille toimivaltaisille valvontaviranomaisille.”

c) korvataan 3 ja 4 kohta seuraavasti:

”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, valvontaelin voi erityisesti laiminlyönnin laajuuden, keston ja seuraukset huomioon ottaen perua kyseisen palveluntarjoajan tai sen tarjoaman kyseessä olevan palvelun hyväksytyn aseman.

3 a. Jos direktiivissä (EU) XXXX/XXXX [NIS2-direktiivi] tarkoitetut kansalliset toimivaltaiset viranomaiset ilmoittavat valvontaelimelle, että hyväksytty luottamuspalvelun tarjoaja ei täytä jotain direktiivin (EU) XXXX/XXXX [NIS2-direktiivi] 18 artiklassa säädetyistä vaatimuksista, valvontaelin voi erityisesti laiminlyönnin laajuuden, keston ja seuraukset huomioon ottaen perua kyseisen palveluntarjoajan tai sen tarjoaman kyseessä olevan palvelun hyväksytyn aseman.

3 b. Jos asetuksessa (EU) 2016/679 tarkoitetut valvontaviranomaiset ilmoittavat valvontaelimelle, että hyväksytty luottamuspalvelun tarjoaja ei täytä jotain asetuksessa (EU) 2016/679 säädetyistä vaatimuksista, valvontaelin voi erityisesti laiminlyönnin laajuuden, keston ja seuraukset huomioon ottaen perua kyseisen palveluntarjoajan tai sen tarjoaman kyseessä olevan palvelun hyväksytyn aseman.

3 c. Valvontaelimen on ilmoitettava hyväksytylle luottamuspalvelun tarjoajalle sen hyväksytyn aseman tai kyseessä olevan palvelun hyväksytyn aseman perumisesta. Valvontaelimen on ilmoitettava asiasta 22 artiklan 3 kohdassa tarkoitetulle elimelle 22 artiklan 1 kohdassa tarkoitettujen luotettujen luetteloiden päivittämistä varten ja direktiivissä XXXX [NIS2-direktiivi] tarkoitetulle kansalliselle toimivaltaiselle viranomaiselle.

4. Komissio vahvistaa 12 kuukauden kuluessa tämän asetuksen voimaantulosta tekniset eritelmät ja standardien viitenumerot antamalla täytäntöönpanosäädöksiä seuraavilta osin:

a) edellä 1 kohdassa tarkoitettu vaatimustenmukaisuuden arviointilaitosten akkreditointi ja vaatimustenmukaisuuden arviointikertomus;

b) tarkastusvaatimukset, joiden mukaisesti vaatimustenmukaisuuden arviointilaitokset suorittavat 1 kohdassa tarkoitetun hyväksyttyjen luottamuspalvelun tarjoajien vaatimustenmukaisuuden arvioinnin;

c) vaatimustenmukaisuuden arviointijärjestelmät, joiden mukaisesti vaatimustenmukaisuuden arviointilaitokset suorittavat hyväksyttyjen luottamuspalvelujen tarjoajien vaatimustenmukaisuuden arvioinnin ja antavat 1 kohdassa tarkoitetun raportin.

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

23) Muutetaan 21 artikla seuraavasti:

”1. Jos luottamuspalvelun tarjoajat aikovat aloittaa hyväksytyn luottamuspalvelun tarjoamisen, niiden on toimitettava valvontaelimelle ilmoitus aikeestaan ja yhdessä sen kanssa vaatimustenmukaisuuden arviointilaitoksen antama vaatimustenmukaisuuden arviointiraportti, jossa vahvistetaan tässä asetuksessa ja direktiivin (EU) XXXX/XXXX [NIS2-direktiivi] 18 artiklassa säädettyjen vaatimusten täyttyminen.”

a) korvataan 2 kohta seuraavasti:

”2. Valvontaelimen on tarkastettava, täyttävätkö luottamuspalvelun tarjoaja ja sen tarjoamat luottamuspalvelut tässä asetuksessa säädetyt vaatimukset ja erityisesti hyväksyttyjä luottamuspalvelun tarjoajia ja niiden tarjoamia hyväksyttyjä luottamuspalveluja koskevat vaatimukset.

Sen tarkastamiseksi, että luottamuspalvelun tarjoaja noudattaa direktiivin XXXX/XXXX [NIS2-direktiivi] 18 artiklassa säädettyjä vaatimuksia, valvontaelimen on pyydettävä direktiivissä XXXX/XXXX [NIS2-direktiivi] tarkoitettuja toimivaltaisia viranomaisia toteuttamaan tältä osin valvontatoimia ja toimittamaan tiedot toimien tuloksista ilman aiheetonta viivytystä kahden kuukauden kuluessa direktiivissä XXXX/XXXX [NIS2-direktiivi] tarkoitettujen toimivaltaisten viranomaisten esittämän pyynnön vastaanottamisesta. Jos tarkastusta ei saada päätökseen kahden kuukauden kuluessa ilmoituksesta, direktiivissä XXXX [NIS2-direktiivi] tarkoitettujen 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 hyväksytty asema sekä ilmoitettava asiasta 22 artiklan 3 kohdassa tarkoitetulle 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 määrittelee 12 kuukauden kuluessa tämän asetuksen voimaantulosta 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.”

25) 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.

Hyväksytyn luottamuspalvelun tarjoajan on tarkastettava ensimmäisessä alakohdassa tarkoitetut tiedot joko suoraan tai kolmatta osapuolta käyttäen millä tahansa seuraavista tavoista:

a) käyttäen eurooppalaista digitaalisen identiteetin lompakkoa tai ilmoitettua sähköisen tunnistamisen menetelmää, joka täyttää 8 artiklassa säädetyt korkeaa varmuustasoa koskevat vaatimukset;

b) käyttäen hyväksyttyä sähköistä attribuuttitodistusta tai 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 asianmukaisia menettelyjä noudattaen ja kansallisen lainsäädännön mukaisesti.”

b) lisätään 1 a kohta seuraavasti:

”1 a. Komissio määrittelee 12 kuukauden kuluessa tämän asetuksen voimaantulosta tekniset vähimmäiseritelmät, -standardit ja -menettelyt 1 kohdan c alakohdan mukaista henkilöllisyyden ja attribuuttien tarkastamista varten antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

c) muutetaan 2 kohta seuraavasti:

0) muutetaan a alakohta seuraavasti:

”a) ilmoitettava valvontaelimelle vähintään kuukautta aikaisemmin, ennen kuin se toteuttaa muutoksia hyväksyttyjen luottamuspalvelujensa tarjoamiseen, tai vähintään kolme kuukautta aikaisemmin, jos tarkoituksena on lopettaa kyseinen toiminta. Valvontaelin voi pyytää lisätietoja tai vaatimustenmukaisuuden arvioinnin tulosta ennen kuin se myöntää luvan toteuttaa suunnitellut muutokset hyväksyttyihin luottamuspalveluihin. 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 saatava päätökseen.”

1) korvataan d ja e alakohta seuraavasti:

”d) ilmoitettava ennen sopimussuhteen aloittamista julkisesti käytettävissä olevassa tilassa ja henkilökohtaisesti henkilöille, jotka haluavat käyttää hyväksyttyä 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 salausalgoritmien, avaimen pituuksien ja hajautusfunktioiden käyttö järjestelmissä, tuotteissa ja niiden tukemissa prosesseissa;”

2) lisätään fa ja fb alakohta seuraavasti:

”fa) noudatettava asianmukaisia toimintaperiaatteita ja toteutettava vastaavat toimenpiteet hyväksyttyjen luottamuspalvelujen tarjoamiseen kohdistuvien oikeudellisten, liiketoiminnallisten, operatiivisten ja muiden suorien tai välillisten riskien hallitsemiseksi. Sen estämättä, mitä direktiivin XXXX/XXX [NIS2-direktiivi] 18 artiklassa säädetään, näihin toimenpiteisiin on sisällyttävä vähintään seuraavat:

i) palveluun rekisteröitymiseen ja asiakassuhteen perustamismenettelyihin liittyvät toimenpiteet;

ii) menettelyllisiin tai hallinnollisiin tarkastuksiin liittyvät toimenpiteet;

iii) palvelujen hallinnointiin ja toteuttamiseen liittyvät toimenpiteet.

fb) 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 siitä, kun ne ovat tulleet asiasta tietoisiksi, palvelujen tarjoamisessa tai fa alakohdan i, ii ja iii alakohdassa tarkoitettujen toimenpiteiden toteuttamisessa havaituista rikkomisista tai häiriöistä, joilla on merkittävä vaikutus tarjottuun luottamuspalveluun tai siinä säilytettyihin henkilötietoihin.”

3) korvataan g ja h alakohta seuraavasti:

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

4) kumotaan j alakohta;

d) lisätään 4 a kohta seuraavasti:

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

e) korvataan 5 kohta seuraavasti:

”5. Komissio vahvistaa 12 kuukauden kuluessa tämän asetuksen voimaantulosta 2 kohdassa tarkoitettuihin vaatimuksiin sovellettavat tekniset eritelmät, menettelyt ja standardien viitenumerot antamalla täytäntöönpanosäädöksiä. Jos näitä teknisiä eritelmiä, menettelyjä ja standardeja noudatetaan, tässä artiklassa säädettyjen vaatimusten katsotaan täyttyvän. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

f) lisätään 6 kohta seuraavasti:

”6. Siirretään komissiolle valta antaa täytäntöönpanosäädöksiä, joissa täsmennetään 2 kohdan fa alakohdassa tarkoitettujen toimenpiteiden teknisiä ominaisuuksia.”

25 a) Muutetaan 26 artikla seuraavasti:

”2. Komissio vahvistaa 12 kuukauden kuluessa tämän asetuksen voimaantulosta kehittyneisiin sähköisiin allekirjoituksiin sovellettavat tekniset eritelmät ja standardien viitenumerot antamalla täytäntöönpanosäädöksiä. Kehittyneitä sähköisiä allekirjoituksia koskevien vaatimusten katsotaan täyttyvän, kun kehittynyt sähköinen allekirjoitus on kyseisten eritelmien ja standardien mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

25 b) Muutetaan 27 artikla seuraavasti:

kumotaan 4 kohta.

26) Korvataan 28 artiklan 6 kohta seuraavasti:

”6. Komissio vahvistaa 12 kuukauden kuluessa tämän asetuksen voimaantulosta sähköisen allekirjoituksen hyväksyttyihin varmenteisiin sovellettavat tekniset eritelmät ja standardien viitenumerot antamalla täytäntöönpanosäädöksiä. Jos sähköisen allekirjoituksen hyväksytty varmenne vastaa kyseisiä eritelmiä ja standardeja, sen katsotaan olevan liitteessä I säädettyjen vaatimusten mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

27) Lisätään 29 artiklaan uusi 1 a kohta seuraavasti:

”1 a. Allekirjoittajan puolesta tapahtuvasta sähköisen allekirjoituksen luontitietojen muodostamisesta, hallinnoinnista tai tällaisten sähköisen allekirjoituksen luontitietojen kahdentamisesta varmuuskopiointitarkoituksiin voi vastata ainoastaan hyväksytty luottamuspalvelun tarjoaja, joka tarjoaa hyväksyttyä luottamuspalvelua hyväksytyn sähköisen allekirjoituksen etäluontivälineen hallinnointia varten.”

28) Lisätään 29 a artikla seuraavasti:

”*29 a artikla*

Hyväksytyn sähköisen allekirjoituksen etäluontivälineiden hallinnoinnin hyväksyttyä palvelua koskevat vaatimukset

1. Hyväksytyn sähköisen allekirjoituksen etäluontivälineen hallinnoinnista hyväksyttynä palveluna voi vastata ainoastaan hyväksytty luottamuspalvelun tarjoaja, joka

   a) muodostaa tai hallinnoi sähköisen allekirjoituksen luontitietoja allekirjoittajan puolesta;

   b) sen estämättä, mitä liitteessä II olevan 1 kohdan d alakohdassa säädetään, saa 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 vaatimukset, jotka on määritetty 30 artiklan nojalla annetussa yksittäisen hyväksytyn allekirjoituksen etäluontivälineen sertifiointiraportissa.

2. Komissio vahvistaa 12 kuukauden kuluessa tämän asetuksen voimaantulosta 1 kohdan vaatimuksiin sovellettavat tekniset eritelmät ja standardien viitenumerot antamalla täytäntöönpanosäädöksiä.”

29) Lisätään 30 artiklaan 3 a kohta seuraavasti:

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

30) Korvataan 31 artiklan 3 kohta seuraavasti:

”3. Komissio määrittelee 12 kuukauden kuluessa tämän asetuksen voimaantulosta 1 kohdan vaatimuksiin liittyvät muotoseikat 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 hyväksyttyjen sähköisten allekirjoitusten validointi vastaa 3 kohdassa tarkoitettuja eritelmiä ja standardeja, sen katsotaan olevan ensimmäisessä alakohdassa säädettyjen vaatimusten mukainen.”

b) korvataan 3 kohta seuraavasti:

”3. Komissio antaa 12 kuukauden kuluessa tämän asetuksen voimaantulosta hyväksyttyjen sähköisten allekirjoitusten validointiin sovellettavat eritelmät ja standardien viitenumerot antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

31 a) Lisätään 32 a artikla seuraavasti:

”Hyväksyttyihin varmenteisiin perustuvien kehittyneiden sähköisten allekirjoitusten validointia koskevat vaatimukset

1. Hyväksyttyyn varmenteeseen perustuvan kehittyneen sähköisen allekirjoituksen validointiprosessilla vahvistetaan hyväksyttyyn varmenteeseen perustuvan kehittyneen sähköisen allekirjoituksen pätevyys, edellyttäen että:

a) allekirjoitusta tukeva varmenne oli allekirjoitushetkellä liitteen I mukainen hyväksytty sähköisen allekirjoituksen varmenne;

b) hyväksytyn varmenteen 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 salanimeä, sen käytöstä on selkeästi ilmoitettu luottavalle osapuolelle;

f) allekirjoitettujen tietojen eheyttä ei ole loukattu;

g) edellä 26 artiklassa säädetyt vaatimukset täyttyivät allekirjoitushetkellä. Jos hyväksyttyihin varmenteisiin perustuvien kehittyneiden sähköisten allekirjoitusten validointi vastaa 3 kohdassa tarkoitettuja eritelmiä ja standardeja, sen katsotaan olevan ensimmäisessä alakohdassa säädettyjen vaatimusten mukainen.

2. Hyväksyttyyn 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 antaa 12 kuukauden kuluessa tämän asetuksen voimaantulosta hyväksyttyihin varmenteisiin perustuvien kehittyneiden sähköisten allekirjoitusten validointiin sovellettavat eritelmät ja standardien viitenumerot antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

31 b) Muutetaan 33 artikla seuraavasti:

”1. Hyväksyttyjen sähköisten allekirjoitusten hyväksyttyä validointipalvelua voi tarjota ainoastaan hyväksytty luottamuspalvelun tarjoaja, joka:”

”2. Komissio vahvistaa 12 kuukauden kuluessa tämän asetuksen voimaantulosta 1 kohdassa tarkoitettuun hyväksyttyyn validointipalveluun sovellettavat tekniset eritelmät ja sitä koskevien standardien viitenumerot antamalla täytäntöönpanosäädöksiä. Jos hyväksyttyjen sähköisten allekirjoitusten validointipalvelu vastaa kyseisiä eritelmiä ja standardeja, sen katsotaan olevan 1 kohdassa säädettyjen vaatimusten mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

32) Korvataan 34 artikla seuraavasti:

”34 artikla

Hyväksyttyjen sähköisten allekirjoitusten hyväksytty säilyttämispalvelu

1. Hyväksyttyjen sähköisten allekirjoitusten hyväksyttyä säilyttämispalvelua voi tarjota ainoastaan hyväksytty luottamuspalvelun tarjoaja, jonka käyttämät menettelyt ja teknologiat ovat sellaisia, että niillä voidaan jatkaa hyväksytyn sähköisen allekirjoituksen luotettavuutta senkin jälkeen, kun niiden teknologinen luotettavuusaika on päättynyt.

2. Jos hyväksyttyjen sähköisten allekirjoitusten hyväksyttyä säilyttämispalvelua koskevat järjestelyt vastaavat 3 kohdassa tarkoitettuja eritelmiä ja standardeja, niiden katsotaan olevan 1 kohdassa säädettyjen vaatimusten mukaisia.

3. Komissio vahvistaa 12 kuukauden kuluessa tämän asetuksen voimaantulosta hyväksyttyjen sähköisten allekirjoitusten hyväksyttyä säilyttämispalvelua koskevat tekniset eritelmät ja standardien viitenumerot antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

32 a) Lisätään 36 artiklaan uusi 2 kohta seuraavasti:

”2. Komissio vahvistaa 12 kuukauden kuluessa tämän asetuksen voimaantulosta kehittyneisiin sähköisiin leimoihin sovellettavien standardien tekniset eritelmät ja viitenumerot antamalla täytäntöönpanosäädöksiä.

Kehittyneitä sähköisiä leimoja koskevien vaatimusten katsotaan täyttyvän, kun kehittynyt sähköinen leima on kyseisten eritelmien ja standardien mukainen. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

33) Muutetaan 37 artikla seuraavasti:

kumotaan 4 kohta.

34) Muutetaan 38 artikla seuraavasti:

a) korvataan 1 kohta seuraavasti:

”1. Sähköisten leimojen hyväksyttyjen varmenteiden on täytettävä liitteessä III säädetyt vaatimukset. Jos sähköisen leiman hyväksytty varmenne vastaa 6 kohdassa tarkoitettuja eritelmiä ja standardeja, sen katsotaan olevan liitteessä III säädettyjen vaatimusten mukainen.”

b) korvataan 6 kohta seuraavasti:

”6. Komissio vahvistaa 12 kuukauden kuluessa tämän asetuksen voimaantulosta sähköisten leimojen hyväksyttyihin varmenteisiin sovellettavat tekniset eritelmät ja standardien viitenumerot antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

35) Lisätään 39 a artikla seuraavasti:

”39 a artikla

Hyväksytyn sähköisen leiman etäluontivälineiden hallinnoinnin hyväksyttyä palvelua koskevat vaatimukset

Hyväksytyn sähköisen leiman etäluontivälineiden hallinnointiin hyväksyttyyn palveluun sovelletaan soveltuvin osin 29 a artiklaa.”

35 a) Lisätään 40 a artikla seuraavasti:

”40 a artikla

Hyväksyttyihin varmenteisiin perustuvien kehittyneiden sähköisten leimojen validointia koskevat vaatimukset

(1) Edellä olevaa 32 a artiklaa sovelletaan soveltuvin osin hyväksyttyihin varmenteisiin perustuvien kehittyneiden sähköisten leimojen validointiin.”

36) Muutetaan 42 artikla seuraavasti:

a) lisätään 1 a kohta seuraavasti:

”1 a. Jos päivän ja ajankohdan sitominen tietoihin ja virheetön aikalähde vastaavat 2 kohdassa tarkoitettuja eritelmiä ja standardeja, niiden katsotaan olevan 1 kohdassa säädettyjen vaatimusten mukaiset.”

b) korvataan 2 kohta seuraavasti:

”2. Komissio vahvistaa 12 kuukauden kuluessa tämän asetuksen voimaantulosta päivän ja ajankohdan sitomista tietoihin sekä virheettömiä aikalähteitä koskevat tekniset eritelmät ja standardien viitenumerot antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

36 a) Lisätään 43 artiklaan uusi 3 kohta seuraavasti:

”2 a. Yhden jäsenvaltion hyväksytty sähköinen rekisteröity jakelupalvelu on tunnustettava hyväksytyksi sähköiseksi rekisteröidyksi jakelupalveluksi kaikissa jäsenvaltioissa.”

37) Muutetaan 44 artikla seuraavasti:

a) lisätään 1 a kohta seuraavasti:

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

b) korvataan 2 kohta seuraavasti:

”2. Komissio vahvistaa 12 kuukauden kuluessa tämän asetuksen voimaantulosta tietojen lähettämis- ja vastaanottamisprosesseihin sovellettavat tekniset eritelmät ja niitä koskevien standardien viitenumerot antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

c) lisätään 3 ja 4 kohta seuraavasti:

”3. Hyväksyttyjen sähköisten rekisteröityjen jakelupalvelujen tarjoajat voivat sopia tarjoamiensa hyväksyttyjen sähköisten rekisteröityjen jakelupalvelujen välisestä yhteentoimivuudesta. Tällaisen yhteentoimivuuskehyksen on oltava 1 kohdassa säädettyjen vaatimusten mukainen. Vaatimustenmukaisuuden arviointilaitoksen on vahvistettava vaatimustenmukaisuus.”

”4. Komissio voi täytäntöönpanosäädöksellä vahvistaa tekniset eritelmät ja standardien viitenumerot helpottaakseen tiedonsiirtoa kahden tai useamman hyväksytyn luottamuspalvelun tarjoajan välillä. Teknisten eritelmien ja standardien sisällön on oltava kustannustehokkaita ja oikeasuhteisia. Täytäntöönpanosäädös hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

38) Korvataan 45 artikla seuraavasti:

”45 artikla

Verkkosivustojen todentamisen hyväksyttyjä varmenteita koskevat vaatimukset

1. Verkkosivustojen todentamisen hyväksyttyjen varmenteiden on täytettävä liitteessä IV säädetyt vaatimukset. Liitteessä IV säädettyjen vaatimusten noudattamista arvioidaan 4 kohdassa tarkoitettujen eritelmien ja standardien mukaisesti.

2. Verkkoselainten on tunnustettava 1 kohdassa tarkoitetut verkkosivustojen todentamisen hyväksytyt varmenteet. Tätä varten verkkoselainten on varmistettava, että millä tahansa menetelmillä annetut henkilötiedot esitetään käyttäjäystävällisellä tavalla. Verkkoselainten on varmistettava tuki 1 kohdassa tarkoitetuille verkkosivustojen todentamisen hyväksytyille varmenteille ja yhteentoimivuus niiden kanssa, lukuun ottamatta yrityksiä, joita pidetään mikroyrityksinä ja pieninä yrityksinä komission suosituksen 2003/361/EY mukaisesti viiden ensimmäisen vuoden aikana, joina ne toimivat verkkoselainpalvelujen tarjoajina.

4. Komissio vahvistaa 12 kuukauden kuluessa tämän asetuksen voimaantulosta 1 ja 2 kohdassa tarkoitettuihin verkkosivustojen todentamisen hyväksyttyihin varmenteisiin sovellettavat eritelmät ja niitä koskevien standardien viitenumerot antamalla täytäntöönpanosäädöksiä. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

39) Lisätään 45 artiklan jälkeen 9, 10 ja 11 jakso seuraavasti:

”9 JAKSO

SÄHKÖINEN ATTRIBUUTTITODISTUS

45 a artikla

Sähköisen attribuuttitodistuksen oikeusvaikutukset

1. Sähköisen attribuuttitodistuksen oikeusvaikutuksia ja käytettävyyttä todisteena oikeudellisissa menettelyissä ei voida kieltää pelkästään sen takia, että se on sähköisessä muodossa tai että se ei täytä hyväksyttyjen sähköisten attribuuttitodistusten vaatimuksia.

2. Hyväksytyllä sähköisellä attribuuttitodistuksella ja virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämillä tai sen puolesta myönnetyillä attribuuttitodistuksilla on sama oikeusvaikutus kuin laillisesti paperimuodossa myönnetyillä todistuksilla.

3. Yhdessä jäsenvaltiossa myönnetty hyväksytty sähköinen attribuuttitodistus on tunnustettava hyväksytyksi sähköiseksi attribuuttitodistukseksi kaikissa jäsenvaltioissa.

4. Virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämä tai sen puolesta myönnetty attribuuttitodistus on tunnustettava kaikissa jäsenvaltioissa virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämäksi tai sen puolesta myönnetyksi attribuuttitodistukseksi.

45 b 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 myönnetyt hyväksytyt sähköiset attribuuttitodistukset.

45 c artikla

Hyväksyttyjä sähköisiä attribuuttitodistuksia koskevat vaatimukset

1. Hyväksyttyjen sähköisten attribuuttitodistusten on täytettävä liitteessä V säädetyt vaatimukset.

1 a. Liitteessä V säädettyjen vaatimusten noudattamista arvioidaan 4 kohdassa tarkoitettujen eritelmien ja standardien mukaisesti.

2. Hyväksytyille sähköisille attribuuttitodistuksille ei saa asettaa muita pakollisia vaatimuksia liitteessä V säädettyjen vaatimusten lisäksi.

3. Jos hyväksytty sähköinen attribuuttitodistus on peruttu sen ensimmäisen myöntämisen jälkeen, sen voimassaolo päättyy peruuttamisajankohdasta lähtien, eikä sen tilaa voida missään olosuhteissa palauttaa.

4. Komissio määrittelee kuuden kuukauden kuluessa tämän asetuksen voimaantulosta hyväksyttyihin sähköisiin attribuuttitodistuksiin sovellettavat tekniset eritelmät ja niitä koskevien standardien viitenumerot antamalla 6 a artiklan 11 kohdassa tarkoitetun eurooppalaisen digitaalisen identiteetin lompakon toteuttamista koskevan täytäntöönpanosäädöksen.

45 d artikla

Attribuuttien tarkastaminen virallisista lähteistä

1. Jäsenvaltioiden on varmistettava 24 kuukauden kuluessa 6 a artiklan 11 kohdassa ja 6 c artiklan 4 kohdassa tarkoitettujen täytäntöönpanosäädösten voimaantulosta, että ainakin liitteessä VI lueteltujen attribuuttien osalta toteutetaan toimenpiteitä, joiden avulla sähköisten attribuuttitodistusten hyväksytyt tarjoajat voivat käyttäjän pyynnöstä ja kansallisen tai unionin lainsäädännön mukaisesti tarkastaa nämä attribuutit sähköisesti, jos nämä attribuutit perustuvat julkisen sektorin virallisiin lähteisiin.

2. Komissio määrittelee kuuden kuukauden kuluessa tämän asetuksen voimaantulosta attribuuttien ja järjestelmien luetteloon perustuvat tekniset vähimmäiseritelmät, -standardit ja -menettelyt attribuuttitodistusten myöntämiselle ja hyväksyttyjen sähköisten attribuuttitodistusten tarkastamiselle, ottaen huomioon asiaa koskevat kansainväliset standardit, antamalla 6 a artiklan 11 kohdassa tarkoitetun eurooppalaisen digitaalisen identiteetin lompakon toteuttamista koskevan täytäntöönpanosäädöksen.

45 da 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) liitteessä VII olevassa b alakohdassa tarkoitetuksi myöntäjäksi nimetyn, 3 artiklan 45 a alakohdassa tarkoitetun julkisen sektorin elimen hyväksyttyä sähköistä allekirjoitusta tai hyväksyttyä sähköistä leimaa tukevan hyväksytyn varmenteen on sisällettävä tietyt automaattiseen käsittelyyn soveltuvassa muodossa olevat varmennetut attribuutit, joissa:

i) ilmoitetaan, että todistuksen myöntävä elin on perustettu kansallisen tai unionin 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; sekä

iii) määritellään i alakohdassa tarkoitettu kansallinen tai unionin lainsäädäntö.

2. Jäsenvaltion, johon 3 artiklan 45 a alakohdassa tarkoitetut julkisen sektorin elimet ovat sijoittautuneet, on varmistettava, että sähköisiä attribuuttitodistuksia myöntävät julkisen sektorin elimet ovat yhtä luotettavia kuin 24 artiklan mukaisesti hyväksytyt luottamuspalvelun tarjoajat.

2 a. Jäsenvaltioiden on ilmoitettava komissiolle 3 artiklan 45 a alakohdassa tarkoitetut julkisen sektorin elimet. 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 45 a alakohdassa tarkoitetuista julkisen sektorin elimistä sähköisesti allekirjoitetussa tai leimatussa muodossa, joka soveltuu automaattiseen käsittelyyn.

3. 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. Peruuttamisen jälkeen sähköisen todistuksen peruutettua tilaa ei voida palauttaa.

4. Virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämän tai sen puolesta myönnetyn sähköisen attribuuttitodistuksen katsotaan olevan tämän artiklan 1 kohdassa säädettyjen vaatimusten mukainen, jos se täyttää 5 kohdassa tarkoitetut standardit.

5. Komissio määrittelee kuuden kuukauden kuluessa tämän asetuksen voimaantulosta virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämiin tai sen puolesta myönnettyihin sähköisiin attribuuttitodistuksiin sovellettavat tekniset eritelmät ja niitä koskevien standardien viitenumerot antamalla 6 a artiklan 11 kohdassa tarkoitetun eurooppalaisen digitaalisen identiteetin lompakon toteuttamista koskevan täytäntöönpanosäädöksen.

5 a. Komissio määrittelee kuuden kuukauden kuluessa tämän asetuksen voimaantulosta 2 a kohdan soveltamiseen liittyvät muotoseikat, menettelyt, eritelmät ja standardit antamalla 6 a artiklan 11 kohdassa tarkoitetun eurooppalaisen digitaalisen identiteetin lompakon toteuttamista koskevan täytäntöönpanosäädöksen.

6. Sähköisten attribuuttitodistusten 3 artiklan 45 a alakohdassa tarkoitettujen myöntäjien on tarjottava rajapinta 6 a artiklan mukaisesti tarjottuihin eurooppalaisiin digitaalisen identiteetin lompakoihin.

45 e artikla

Sähköisten attribuuttitodistusten myöntäminen eurooppalaisiin digitaalisen identiteetin lompakoihin

Hyväksyttyjen sähköisten attribuuttitodistusten tarjoajien on tarjottava rajapinta 6 a artiklan mukaisesti tarjottuihin eurooppalaisiin digitaalisen identiteetin lompakoihin.

45 f artikla

Sähköisiin attribuuttitodistuksiin liittyvien palvelujen tarjoamista koskevat lisäsäännöt

1. Hyväksyttyihin ja ei-hyväksyttyihin sähköisiin attribuuttitodistuksiin liittyvien palvelujen tarjoajat eivät saa yhdistää kyseisten palvelujen tarjoamiseen liittyviä henkilötietoja muista tarjoamistaan tai niiden kauppakumppaneiden tarjoamista palveluista saamiinsa henkilötietoihin.

2. Sähköisiin attribuuttitodistuksiin liittyvien palvelujen tarjoamiseen liittyvät henkilötiedot on pidettävä loogisesti erillään muista sähköisten attribuuttitodistusten tarjoajien hallussa olevista tiedoista.

4. Hyväksyttyihin sähköisiin attribuuttitodistuksiin liittyvien palvelujen tarjoajien on toteutettava toiminnallinen erottelu tällaisten palvelujen tarjoamiseksi.

10 JAKSO

SÄHKÖISET ARKISTOINTIPALVELUT

45 g artikla

Sähköisen arkistointipalvelun oikeusvaikutukset

1. Sähköistä arkistointipalvelua käyttäen tallennettujen sähköisten tietojen oikeusvaikutuksia ja käytettävyyttä todisteena oikeudellisissa menettelyissä ei voida kieltää pelkästään sillä perusteella, että ne ovat sähköisessä muodossa tai että niitä ei ole tallennettu käyttäen hyväksyttyä sähköistä arkistointipalvelua.

2. Hyväksyttyä sähköistä arkistointipalvelua käyttäen tallennettuihin sähköisiin tietoihin sovelletaan olettamaa tietojen eheydestä ja alkuperästä koko sen ajan, jonka ne ovat hyväksytyn luottamuspalvelun tarjoajan säilytettävinä.

3. Yhden jäsenvaltion hyväksytty sähköinen arkistointipalvelu on tunnustettava hyväksytyksi sähköiseksi arkistointipalveluksi kaikissa jäsenvaltioissa.

45 ga artikla

Hyväksyttyjä sähköisiä arkistointipalveluja koskevat vaatimukset

1. Hyväksyttyjen sähköisten arkistointipalvelujen on täytettävä seuraavat vaatimukset:

   a) niitä tarjoavat hyväksytyt luottamuspalvelun tarjoajat;

   b) ne käyttävät menettelyjä ja teknologioita, joilla sähköisten tietojen pysyvyyttä ja luettavuutta voidaan jatkaa teknologista luotettavuusaikaa pidemmälle ja ainakin koko lakisääteisen tai sopimusperusteisen säilytysajan ja säilyttää samalla tietojen eheys ja alkuperä;

c) ne varmistavat, että sähköiset tiedot säilytetään siten, että ne suojataan häviämiseltä ja muuttumiselta, lukuun ottamatta niiden tallennusvälinettä tai sähköistä muotoa koskevia muutoksia;

d) ne antavat valtuutetuille luottaville osapuolille mahdollisuuden saada automaattisesti ilmoitus, jolla vahvistetaan, että hyväksytystä sähköisestä arkistosta haettaviin sähköisiin tietoihin sovelletaan olettamaa tietojen eheydestä säilyttämisajan alusta hakuhetkeen asti. Tämä ilmoitus toimitetaan luotettavalla ja tehokkaalla tavalla, ja siinä on hyväksytyn sähköisen arkistointipalvelun tarjoajan hyväksytty sähköinen allekirjoitus tai hyväksytty sähköinen leima.

2. Komissio vahvistaa 12 kuukauden kuluessa tämän asetuksen voimaantulosta hyväksyttyihin sähköisiin arkistointipalveluihin sovellettavat tekniset eritelmät ja niitä koskevien standardien viitenumerot antamalla täytäntöönpanosäädöksiä. Hyväksyttyjä sähköisiä arkistointipalveluja koskevien vaatimusten katsotaan täyttyvän, kun hyväksytty sähköinen arkistointipalvelu täyttää kyseiset eritelmät ja standardit. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

11 JAKSO

SÄHKÖISET TILIKIRJAT

45 h artikla

Sähköisten tilikirjojen oikeusvaikutukset

1. Sähköisen tilikirjan oikeusvaikutuksia ja käytettävyyttä todisteena oikeudellisissa menettelyissä ei voida kieltää pelkästään sillä perusteella, että se on sähköisessä muodossa tai että se ei täytä hyväksyttyjen sähköisten tilikirjojen vaatimuksia.

2. Hyväksytyn sähköisen tilikirjan tietoihin liitetään olettama, jonka mukaan ne ovat yksilöllisessä ja oikeellisessa peräkkäisessä kronologisessa järjestyksessä ja eheitä.

3. Yhden jäsenvaltion hyväksytty sähköinen tilikirja on tunnustettava hyväksytyksi sähköiseksi tilikirjaksi kaikissa jäsenvaltioissa.

45 i artikla

Hyväksyttyjä sähköisiä tilikirjoja koskevat vaatimukset

1. Hyväksyttyjen sähköisten tilikirjojen on täytettävä seuraavat vaatimukset:

   a) ne luo yksi tai useampi hyväksytty luottamuspalvelun tarjoaja;

   b) ne vahvistavat tilikirjassa olevien tietojen alkuperän;

   c) ne varmistavat tilikirjan tietojen 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 eritelmiä ja standardeja, sen katsotaan olevan 1 kohdassa säädettyjen vaatimusten mukainen.

3. Komissio vahvistaa täytäntöönpanosäädöksin hyväksyttyjen sähköisten tilikirjojen luomiseen ja toimintaan sovellettavat tekniset eritelmät ja niitä koskevien standardien viitenumerot. Nämä täytäntöönpanosäädökset hyväksytään 48 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

40. Lisätään 48 a artikla seuraavasti:

”*48 a artikla*

Raportointivaatimukset

1. Jäsenvaltioiden on varmistettava, että eurooppalaisten digitaalisen identiteetin lompakoiden 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) tiivistelmäraportti, joka sisältää tiedot eurooppalaisen digitaalisen identiteetin lompakon käytön estävistä poikkeamista.

3. Edellä 2 kohdassa tarkoitetut tilastotiedot on julkaistava avoimessa ja yleisesti käytetyssä koneellisesti luettavassa muodossa.

4. Jäsenvaltioiden on toimitettava komissiolle kunkin vuoden 31 päivään maaliskuuta mennessä kertomus 2 kohdan mukaisesti kerätyistä tilastoista.”

41. Korvataan 49 artikla seuraavasti:

”49 artikla

Uudelleentarkastelu

1. Komissio tarkastelee uudelleen tämän asetuksen soveltamista ja antaa Euroopan parlamentille ja neuvostolle kertomuksen 36 kuukauden kuluessa asetuksen voimaantulosta. Komissio arvioi erityisesti 6 artiklan ja 6 db artiklan soveltamisalaa ja sitä, olisiko tämän asetuksen tai sen tiettyjen säännösten soveltamisalaa asianmukaista muuttaa, ottaen huomioon tämän asetuksen soveltamisesta saatu kokemus sekä kuluttajakysyntään ja markkinoihin liittyvä sekä tekninen ja oikeudellinen kehitys. Kertomukseen liitetään tarvittaessa tämän asetuksen muuttamista koskeva ehdotus.

2. Arviointikertomukseen on sisällyttävä arvio tämän asetuksen soveltamisalaan kuuluvien eurooppalaisten digitaalisen identiteetin lompakoiden saatavuudesta ja käytettävyydestä sekä arvio siitä, onko kaikille yksityisille verkkopalvelujen tarjoajille, jotka käyttävät kolmannen osapuolen tarjoamia sähköisen tunnistamisen palveluja käyttäjien todentamista varten, annettava velvoite hyväksyä eurooppalaisten digitaalisen identiteetin lompakoiden käyttö.

3. Lisäksi komissio antaa Euroopan parlamentille ja neuvostolle ensimmäisessä kohdassa tarkoitetun kertomuksen jälkeen neljän vuoden välein kertomuksen edistymisestä tämän asetuksen tavoitteiden saavuttamisessa.”

42. 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 hyväksyttyinä sähköisen allekirjoituksen luontivälineinä 36 kuukauden ajan tämän asetuksen voimaantulosta.

2. Direktiivin 1999/93/EY mukaisesti luonnollisille henkilöille myönnettyjä hyväksyttyjä varmenteita pidetään tämän asetuksen mukaisina sähköisten allekirjoitusten hyväksyttyinä varmenteina 24 kuukauden ajan tämän asetuksen voimaantulosta.

2 a. Niiden hyväksyttyjen luottamuspalvelun tarjoajien hallinnointia, jotka eivät ole hyväksyttyjä luottamuspalveluja hyväksyttyjen sähköisen allekirjoituksen ja leiman etäluontivälineiden hallinnointia varten 29 a ja 39 a artiklan mukaisesti tarjoavia hyväksyttyjä luottamuspalvelun tarjoajia, on edelleen tarkasteltava ilman, että niiden on tarvetta saada hyväksytty asema näiden hallinnointipalvelujen tarjoamiseksi 24 kuukauden ajan tämän asetuksen voimaantulosta.

2 b. Hyväksyttyjen luottamuspalvelun tarjoajien, joille on myönnetty hyväksytty asema tämän asetuksen nojalla ennen [muutosasetuksen voimaantulopäivää] ja jotka käyttävät henkilöllisyyden todentamismenetelmiä hyväksyttyjen varmenteiden myöntämiseksi 24 artiklan 1 kohdan mukaisesti, on toimitettava valvontaelimelle vaatimustenmukaisuuden arviointiraportti, jossa vahvistetaan 24 artiklan 1 kohdan noudattaminen, mahdollisimman pian ja viimeistään 30 kuukauden kuluttua muutosasetuksen voimaantulosta. Hyväksytty luottamuspalvelun tarjoaja voi edelleen käyttää asetuksen (EU) N:o 910/2014 24 artiklan 1 kohdassa säädettyjä henkilöllisyyden todentamismenetelmiä, kunnes kyseinen vaatimustenmukaisuuden arviointiraportti on toimitettu ja valvontaelin on saattanut sen arvioinnin päätökseen.”

43. Muutetaan liite I tämän asetuksen liitteen I mukaisesti.

44. Korvataan liite II tämän asetuksen liitteessä II olevalla tekstillä.

45. Muutetaan liite III tämän asetuksen liitteen III mukaisesti.

46. Muutetaan liite IV tämän asetuksen liitteen IV mukaisesti.

47. Lisätään uusi liite V tämän asetuksen liitteen V mukaisesti.

48. Lisätään uusi liite VI tämän asetuksen liitteen VI mukaisesti.

52 artikla

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	Neuvoston puolesta
Puhemies	Puheenjohtaja

LIITE I

Korvataan liitteessä I oleva i alakohta seuraavasti:

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

LIITE II

HYVÄKSYTTYJÄ SÄHKÖISEN ALLEKIRJOITUKSEN LUONTIVÄLINEITÄ KOSKEVAT VAATIMUKSET

1. Hyväksytyillä sähköisen allekirjoituksen luontivälineillä on tarkoituksenmukaista tekniikkaa ja menettelytapoja käyttäen varmistettava ainakin, että

   a) sähköisen allekirjoituksen luomisessa käytettävien sähköisen allekirjoituksen luontitietojen luottamuksellisuus taataan kohtuudella;

   b) sähköisen allekirjoituksen luomisessa käytettäviä sähköisen allekirjoituksen luontitietoja voi käytännössä esiintyä vain kerran;

   c) sähköisen allekirjoituksen luomisessa käytettävät sähköisen allekirjoituksen luontitiedot eivät kohtuullisella varmuudella ole pääteltävissä ja sähköinen allekirjoitus on luotettavasti suojattu väärentämiseltä kulloinkin saatavilla olevan teknologian mukaisesti;

   d) laillinen allekirjoittaja voi luotettavasti suojata sähköisen allekirjoituksen luomisessa käytettävät sähköisen allekirjoituksen luontitiedot muiden käytöltä.

2. Hyväksytyt sähköisen allekirjoituksen luontivälineet eivät saa muuttaa allekirjoitettavia tietoja eivätkä estää niiden esittämistä allekirjoittajalle ennen allekirjoittamista.

LIITE III

Korvataan liitteessä III oleva i alakohta seuraavasti:

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

LIITE IV

Korvataan liitteessä IV oleva j alakohta seuraavasti:

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

LIITE V

HYVÄKSYTTYJÄ SÄHKÖISIÄ ATTRIBUUTTITODISTUKSIA KOSKEVAT VAATIMUKSET

Hyväksyttyjen sähköisten attribuuttitodistusten on sisällettävä:

e) tieto, ainakin automaattiseen tietojenkäsittelyyn soveltuvassa muodossa, siitä, että todistus on myönnetty hyväksyttynä sähköisenä attribuuttitodistuksena;

f) tietokokonaisuus, joka yksiselitteisesti edustaa hyväksytyn sähköisen attribuuttitodistuksen myöntävää hyväksyttyä luottamuspalvelun tarjoajaa ja sisältää ainakin tiedon jäsenvaltiosta, johon tarjoaja on sijoittautunut, ja

– oikeushenkilön osalta: nimi ja tarvittaessa rekisterinumero virallisissa rekistereissä olevassa muodossa,

– luonnollisen henkilön osalta: henkilön nimi;

g) tietokokonaisuus, joka yksiselitteisesti edustaa tahoa, johon todistetut attribuutit viittaavat; jos käytetään salanimeä, tämä on ilmoitettava selvästi;

h) todistettu attribuutti tai todistetut attribuutit, tarvittaessa mukaan lukien tiedot, jotka ovat tarpeen kyseisten attribuuttien kattavuuden määrittämiseksi;

i) tiedot todistuksen voimassaoloajan alkamisesta ja päättymisestä;

j) todistuksen tunniste, jonka on oltava kyseisen hyväksytyn luottamuspalvelun tarjoajan osalta yksilöivä, ja tarvittaessa tieto todistusjärjestelmästä, jonka osa attribuuttitodistus on;

k) myöntävän hyväksytyn luottamuspalvelun tarjoajan hyväksytty sähköinen allekirjoitus tai hyväksytty sähköinen leima;

l) sijainti, josta g kohdassa tarkoitettua hyväksyttyä sähköistä allekirjoitusta tai hyväksyttyä sähköistä leimaa tukeva varmenne on saatavilla veloituksetta;

m) tieto hyväksytyn todistuksen voimassaolon tilasta tai niiden palvelujen sijainti, joista sen voi selvittää.

LIITE VI

ATTRIBUUTTIEN VÄHIMMÄISLUETTELO

Tämän asetuksen 45 d artiklan mukaisesti jäsenvaltioiden on varmistettava, että toteutetaan toimenpiteitä, joiden avulla sähköisten attribuuttitodistusten hyväksytyt 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 kansallisen tai unionin lainsäädännön mukaisesti, tapauksissa, joissa nämä attribuutit perustuvat julkisen sektorin virallisiin lähteisiin:

1. Osoite
2. Ikä
3. Sukupuoli
4. Siviilisääty
5. Perheen koostumus
6. Kansalaisuus tai kansallisuus
7. Koulutus, oppiarvot ja tutkintotodistukset
8. Ammattipätevyys, ammattinimikkeet ja toimiluvat
9. Julkiset luvat
10. Taloudelliset ja yritystiedot.

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 salanimeä, tämä 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 veloituksetta;
i) tieto todistuksen voimassaolon tilasta tai niiden palvelujen sijainti, joista sen voi selvittää.