Europos Sąjungos
Taryba

Briuselis, 2022 m. gruodžio 6 d.
(OR. en)

15706/22

Tarpinstitucinė byla:
2021/0136(COD)

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

POSĖDŽIO REZULTATAI

nuo:	Tarybos generalinio sekretoriato
data:	2022 m. gruodžio 6 d.
kam:	Delegacijoms
Ankstesnio dokumento Nr.:	14959/22 + ADD 1 + ADD 2
Komisijos dok. Nr.:	9471/21
Dalykas:	Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo dėl Europos skaitmeninės tapatybės sistemos nustatymo iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 – Bendras požiūris (2022 m. gruodžio 6 d.)

Delegacijoms priede pateikiamas Tarybos bendras požiūris dėl pirmiau nurodyto pasiūlymo; Taryba tą bendrą požiūrį patvirtino 3917-ajame Tarybos (transportas, telekomunikacijos ir energetika) posėdyje 2022 m. gruodžio 6 d.

Bendrame požiūryje nustatyta Tarybos preliminari pozicija dėl šio pasiūlymo ir juo remiamasi rengiantis deryboms su Europos Parlamentu.

PRIEDAS

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS

kuriuo dėl Europos skaitmeninės tapatybės sistemos nustatymo iš dalies keičiamas Reglamentas (ES) Nr. 910/2014

EUROPOS PARLAMENTAS IR EUROPOS SĄJUNGOS TARYBA,

atsižvelgdami į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 114 straipsnį,

atsižvelgdami į Europos Komisijos pasiūlymą,

teisėkūros procedūra priimamo akto projektą perdavus nacionaliniams parlamentams,

atsižvelgdami į Europos ekonomikos ir socialinių reikalų komiteto nuomonę[1],

laikydamiesi įprastos teisėkūros procedūros,

kadangi:

(1) 2020 m. vasario 19 d. Komisijos komunikate „Europos skaitmeninės ateities formavimas“[2] skelbiama apie Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 peržiūrą siekiant pagerinti jo veiksmingumą, išplėsti jo teikiamą naudą į privatųjį sektorių ir skatinti naudoti patikimas skaitmenines tapatybes visiems europiečiams;

[1] OL C […], […], p. […].
[2] COM(2020)67 final.

(2) savo 2020 m. spalio 1–2 d. išvadose[3], Europos Vadovų Taryba paragino Komisiją pasiūlyti kurti saugios viešosios elektroninės atpažinties sistemą Sąjungos lygmeniu, įskaitant sąveikius skaitmeninius parašus, kad žmonės galėtų kontroliuoti savo internetinę tapatybę ir duomenis bei galėtų naudotis viešosiomis, privačiosiomis ir tarpvalstybinėmis skaitmeninėmis paslaugomis;

(3) 2021 m. kovo 9 d. Komisijos komunikate „2030 m. skaitmeninės politikos kelrodis: Europos skaitmeninio dešimtmečio kelias“[4] nustatyti Sąjungos sistemos tikslai, kuriais iki 2030 m. siekiama plačiai įdiegti patikimą, naudotojų kontroliuojamą tapatybę, leidžiančią kiekvienam naudotojui kontroliuoti savo veiksmus ir sąveikas internete;

(4) darnesnis požiūris į skaitmeninę atpažintį turėtų sumažinti dabartinio susiskaidymo, kylančio dėl skirtingų nacionalinių sprendimų naudojimo, riziką ir sąnaudas ir stiprins bendrąją rinką sudarydamas sąlygas piliečiams, kitiems gyventojams, kaip apibrėžta nacionalinėje teisėje, ir įmonėms internetu patogiai ir vienodomis sąlygomis įrodyti savo tapatybę visoje Sąjungoje. Europinė skaitmeninės tapatybės dėklė fiziniams ir juridiniams asmenims visoje Sąjungoje suteiks galimybę naudotis suderintomis elektroninės atpažinties priemonėmis, kurios suteiks jiems galimybę nustatyti su jų tapatybe susietų duomenų autentiškumą ir jais dalytis. Visi turėtų turėti galimybę saugiai naudotis viešosiomis ir privačiosiomis paslaugomis pasikliaujant pagerinta patikimumo užtikrinimo paslaugų ekosistema ir patikrintais tapatybės įrodymais bei požymių liudijimais, pvz., visoje Sąjungoje teisiškai pripažįstamu ir priimamu universiteto diplomu. Europos skaitmeninės tapatybės sistema siekiama pereiti nuo kliovimosi tik nacionaliniais skaitmeninės tapatybės sprendimais prie elektroninių požymių liudijimų, kurie galioja Europos lygmeniu, teikimo. Elektroninių požymių liudijimų teikėjams turėtų būti naudingos aiškios ir vienodos taisyklės, o viešojo administravimo institucijos turėtų turėti galimybę kliautis atitinkamo formato elektroniniais dokumentais;

---

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

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

(4a) kai kurios valstybės narės yra įdiegusios ir plačiai naudoja elektroninės atpažinties priemones, kurias šiuo metu pripažįsta paslaugų teikėjai Sąjungoje. Be to, buvo investuojama į nacionalinius ir tarpvalstybinius sprendimus, grindžiamus dabartiniu eIDAS reglamentu, įskaitant eIDAS mazgų sąveikumo techninę infrastruktūrą. Siekiant, kad būtų užtikrintas papildomumas bei tai, kad elektroninės atpažinties priemonių, apie kurias pranešta, dabartiniai naudotojai greitai priimtų europines skaitmeninės tapatybės dėkles, ir kad būtų kuo labiau sumažintas poveikis esamiems paslaugų teikėjams, tikimasi, kad europinių skaitmeninių tapatybės dėklių srityje bus naudinga remtis patirtimi, susijusia su esamomis elektroninės atpažinties priemonėmis, ir pasinaudoti įdiegta eIDAS infrastruktūra Europos ir nacionaliniu lygmenimis;

(5) siekdami remti Europos įmonių konkurencingumą, internetinių paslaugų teikėjai turėtų turėti galimybę pasikliauti visoje Sąjungoje pripažįstamais skaitmeninės tapatybės sprendimais, nepriklausomai nuo valstybės narės, kurioje jie buvo pateikti, taip gaudami naudos iš suderinto europinio požiūrio į patikimumą, saugumą ir sąveikumą. Naudotojai ir paslaugų teikėjai taip pat turėtų turėti galimybę gauti naudos iš tos pačios elektroninių požymių liudijimų teisinės vertės visoje Sąjungoje;

(6) įgyvendinant šį reglamentą asmens duomenų tvarkymui taikomas Reglamentas (ES) Nr. 2016/679[5]. Dėl to šiame reglamente turėtų būti nustatytos konkrečios apsaugos priemonės, kuriomis būtų užtikrinama, kad elektroninės atpažinties priemonių ir elektroninių požymių liudijimų teikėjai negalėtų sujungti kitas paslaugas teikiant gautų asmens duomenų su asmens duomenimis, susijusiais su paslaugomis, kurioms taikomas šis reglamentas; Su europinėmis skaitmeninės tapatybės dėklėmis susiję asmens duomenys turėtų būti saugomi logiškai atskirti nuo bet kokių kitų leidėjo turimų duomenų. Šiuo reglamentu europinių skaitmeninės tapatybės dėklių leidėjams nekliudoma taikyti papildomas technines priemones, kuriomis prisidedama prie asmens duomenų apsaugos, pavyzdžiui, fizinį asmens duomenų, susijusių su dėklių diegimu, atskyrimą nuo bet kokių kitų leidėjo turimų duomenų.

---

5 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas), OL L 119, 2016 5 4, p. 1.

(7) būtina nustatyti suderintas sąlygas dėl europinių skaitmeninės tapatybės dėklių, kurias turi pateikti valstybės narės, sistemos kūrimo – taip visiems ES piliečiams ir kitiems gyventojams, kaip apibrėžta nacionalinėje teisėje, turėtų būti suteikta galių saugiai dalytis su jų tapatybe susijusiais duomenimis naudotojams palankiu ir patogiu būdu prižiūrint vien naudotojui. Šiems tikslams pasiekti naudojamos technologijos turėtų būti kuriamos taip, kad būtų siekiama aukščiausio lygio saugumo, patogumo naudotojams ir plataus masto naudojimo. Valstybės narės visiems savo piliečiams ir gyventojams turėtų užtikrinti vienodas galimybes naudotis skaitmenine atpažintimi;

(8) siekiant užtikrinti, kad pasikliaujančiosios šalys galėtų kliautis europinės skaitmeninės tapatybės dėklių naudojimu ir apsaugoti naudotoją nuo neteisėto neskelbtinų duomenų naudojimo, pasikliaujančiosios šalys turėtų būti registruotos kaip pranešimo proceso dalis. Pasikliaujančiosioms šalims taikomi pranešimo reikalavimai daugeliu atvejų turėtų būti grindžiami riboto kiekio informacijos, kurios reikia, kad pasikliaujančioji šalis galėtų atlikti tapatumo nustatymą, susijusį su europine skaitmeninės tapatybės dėkle, teikimu. Laikantis šių reikalavimų taip pat turėtų būti leidžiama taikyti automatizuotas ar paprastas savarankiško pranešimo procedūras, įskaitant valstybių narių kliovimąsi ir naudojimąsi esamais registrais. Be to, neskelbtinų duomenų kategorijoms nacionaliniu arba Sąjungos lygmeniu gali būti taikoma speciali tvarka, pagal kurią pasikliaujančiosioms šalims gali būti nustatyti griežtesni registravimo ir leidimo suteikimo reikalavimai, kad tokiais atvejais būtų užkirstas kelias neteisėtam tapatybės duomenų naudojimui. Kitais naudojimo atvejais pasikliaujančiosios šalys gali būti atleistos nuo pareigos pranešti apie savo ketinimą kliautis Europos skaitmenine dėkle, pavyzdžiui, kai dėl teisės patikrinti konkrečius požymius nėra reikalaujama ar leidžiama, kad pasikliaujančioji šalis naudodamasi elektroninėmis priemonėmis atliktų tapatumo nustatymą. Paprastai esant šiems fizinį dalyvavimą apimantiems scenarijams, naudotojas gali nustatyti pasikliaujančiąją šalį dėl konteksto, pavyzdžiui, bendraujant su automobilių nuomos darbuotoju arba vaistininku. Pranešimo procesas turi būti grindžiamas sektoriniais Sąjungos arba nacionaliniais teisės aktais, nes taip galima atsižvelgti į įvairius naudojimo atvejus, kurie gali skirtis registracijos reikalavimų, veikimo režimo (internetu ir (arba) ne internetu) arba reikalavimo patvirtinti prietaisų, galinčių turėti sąsają su europine skaitmeninės tapatybės dėkle, tapatumą aspektais. Europinės skaitmeninės tapatybės dėklės lygmeniu neturėtų būti suteikti įgaliojimai užtikrinti Europinės skaitmeninės tapatybės dėklės naudojimo tikrinimą, kurį vykdo pasikliaujančiosios šalys.

(9) visos europinės skaitmeninės tapatybės dėklės turėtų suteikti naudotojams galimybę naudotis elektronine atpažintimi ir tapatumo nustatymu internetu ir ne internetu visose šalyse prieigai prie įvairių viešųjų ir privačių paslaugų. Nepažeidžiant valstybių narių prerogatyvos dėl savo piliečių ir gyventojų atpažinties, dėklėmis gali būti tenkinami instituciniai viešojo administravimo įstaigų, tarptautinių organizacijų ir Sąjungos institucijų, įstaigų, biurų ir agentūrų poreikiai. Daugelyje sektorių, įskaitant sveikatos sektorių, kur paslaugos dažnai teikiamos kontaktiniu būdu, būtų svarbus naudojimas neprisijungus ir e. receptų sistemoje būtų galima kliautis QR kodais ar panašiomis technologijomis tapatumui patikrinti. Kliaujantis aukštu saugumo užtikrinimo lygiu europinėms skaitmeninės tapatybės dėklėms turėtų praversti nuo klastojimo apsaugantys sprendimai, pvz., saugūs elementai, kad būtų vykdomi pagal šį reglamentą keliami saugumo reikalavimai. Europinė skaitmeninės tapatybės dėklė taip pat turėtų naudotojams suteikti galimybę kurti ir naudoti visoje ES priimamus kvalifikuotus elektroninius parašus ir spaudus. Siekdamos naudos visiems ES piliečiams ir įmonėms supaprastinus tvarką ir sumažinus išlaidas, be kita ko, suteikus atstovavimo ir e. įgaliojimų galimybę, valstybės narės turėtų išleisti europines skaitmeninės tapatybės dėkles, pasitelkusios bendruosius standartus, kad užtikrintų sklandų sąveikumą ir aukštą saugumo lygį. Tik valstybių narių kompetentingos institucijos gali suteikti aukšto lygio patikimumą nustatant asmens tapatybę ir taip užtikrinti, kad asmuo, pareiškęs, kad jam priklauso tam tikra tapatybė, ar ją patvirtinęs asmuo iš tiesų yra asmuo, kuriuo jis ar ji teigia esąs. Dėl to būtina, kad naudojantis europinėmis skaitmeninės tapatybės dėklėmis būtų pasikliaujama teisine piliečių, kitų gyventojų ar juridinių subjektų tapatybe. Pasitikėjimą europinėmis skaitmeninės tapatybės dėklėmis stiprintų tai, kad išduodančios šalys turėtų įgyvendinti tinkamas technines ir organizacines priemones, kad užtikrintų, jog saugumo lygis atitinka fizinių asmenų teisėms ir laisvėms kylančią riziką, laikydamosi Reglamento (ES) 2016/679. Fiziniams asmenims europinės skaitmeninės tapatybės dėklės išduodamos, jie jomis naudojasi tapatumui nustatyti ir jos atšaukiamos nemokamai. Paslaugų, kurias teikiant pasikliaujama dėklės naudojimu, atveju gali būti patiriama išlaidų, susijusių, pavyzdžiui, su elektroninių dėklės požymių liudijimų išdavimu;

(9a) naudinga palengvinti europinių skaitmeninės tapatybės dėklių diegimą ir naudojimą, jas sklandžiai integruojant į nacionaliniu, vietos ar regioniniu lygmeniu jau įgyvendinamų viešųjų ir privačiųjų skaitmeninių paslaugų ekosistemą. Šiam tikslui pasiekti valstybės narės gali numatyti teisines ir organizacines priemones, kad europinių skaitmeninės tapatybės dėklių leidėjams būtų suteikta daugiau lankstumo ir kad būtų galima numatyti papildomų europinių skaitmeninės tapatybės dėklių funkcijų, viršijančių tai, kas nustatyta šiame reglamente, be kita ko, užtikrinant didesnį sąveikumą su esamomis nacionalinėmis elektroninės atpažinties priemonėmis. Tai jokiu būdu neturėtų pakenkti pagrindinių europinių skaitmeninės tapatybės dėklių funkcijų, kaip nustatyta šiame reglamente, vykdymui, taip pat neturėtų būti skatinami esami nacionaliniai sprendimai teikiant pirmenybę jiems, o ne europinėms skaitmeninės tapatybės dėklėms. Kadangi šios papildomos funkcijos viršija šio reglamento taikymo sritį, joms netaikomos šiame reglamente išdėstytos nuostatos dėl tarpvalstybinio kliovimosi europinėmis skaitmeninės tapatybės dėklėmis;

(10) siekiant užtikrinti aukštą duomenų apsaugos, saugumo ir patikimumo lygį, šiuo reglamentu turėtų būti nustatyta suderinta sistema, kurioje būtų išsamiai išdėstytos europinėms skaitmeninės tapatybės dėklėms taikomos bendros specifikacijos ir reikalavimai. Europinių skaitmeninės tapatybės dėklių atitiktį tiems reikalavimams turėtų sertifikuoti valstybių narių paskirtos akredituotos atitikties vertinimo įstaigos. Sertifikuojant visų pirma turėtų būti kliaujamasi atitinkamomis Europos kibernetinio saugumo sertifikavimo schemomis ar jų dalimis, nustatytomis pagal Reglamentą (ES) 2019/881[6], tiek, kiek jos apima europinėms skaitmeninės tapatybės dėklėms taikomus kibernetinio saugumo reikalavimus. Kliaujantis Europos kibernetinio saugumo sertifikavimo schemomis turėtų būti užtikrintas suderintas pasitikėjimo europinių skaitmeninės tapatybės dėklių saugumu, nepriklausomai nuo to, kur jos išduotos Sąjungoje, lygis. Europinių skaitmeninės tapatybės dėklių kibernetinio saugumo sertifikavimas turėtų būti grindžiamas nacionalinių kibernetinio saugumo sertifikavimo institucijų vaidmeniu – prižiūrėti ir stebėti jų jurisdikcijai priklausančių atitikties vertinimo įstaigų išduotų sertifikatų atitiktį atitinkamoms Europos kibernetinio saugumo schemoms. Analogiškai, sertifikuojant turėtų būti atitinkamai remiamasi standartais ir techninėmis specifikacijomis, kaip nurodyta Reglamente (ES) 2019/881. Tokios specifikacijos gali būti naudojamos kaip naujausi dokumentai, kaip nurodyta atitinkamose kibernetinio saugumo sertifikavimo schemose pagal Reglamentą (ES) 2019/881. Kai atitinkamos Europos kibernetinio saugumo sertifikavimo schemos, nustatytos pagal Reglamentą (ES) 2019/881, neapima atitinkamų paslaugų ar procesų, kuriais prisidedama prie dėklės saugumo, sertifikavimo, pagal Reglamento (ES) 2019/881 III antraštinę dalį turėtų būti sukurtos atitinkamos schemos. Turėtų būti nustatyta bendra ir suderinta europinių skaitmeninės tapatybės dėklių sertifikavimo schema, pagal kurią būtų vertinama jų atitiktis šiame reglamente nustatytoms bendroms specifikacijoms ir reikalavimams, išskyrus susijusius su kibernetiniu saugumu ir duomenų apsauga, visų pirma tuos, kurie apima funkcinius ir veikimo aspektus. Kalbant apie šį sertifikavimą, siekiant užtikrinti aukšto lygio pasitikėjimą ir skaidrumą, turėtų būti nustatyti mechanizmai ir procedūros, kuriais būtų siekiama skatinti valstybių narių tarpusavio mokymąsi ir bendradarbiavimą sertifikavimo įstaigų ir jų išduodamų sertifikatų bei sertifikavimo ataskaitų stebėsenos ir peržiūros srityje. Toks tarpusavio mokymosi mechanizmas neturėtų daryti poveikio Reglamentui (ES) 2016/679 ir Reglamentui (ES) 2019/881. Dėklės sertifikavimas pagal Reglamentą (ES) 2016/679 yra savanoriška priemonė, kuri gali būti naudojama siekiant įrodyti atitiktį Reglamente (ES) 2016/679 nustatytiems reikalavimams, kai jie taikomi europinėms skaitmeninės tapatybės dėklėms ir jų teikimui Europos piliečiams;

---

[6] 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas), OL L 151, 2019 6 7, p. 15.

(10a) piliečių ir gyventojų prisijungimas prie europinės skaitmeninės tapatybės dėklės turėtų būti palengvintas kliaujantis aukšto saugumo užtikrinimo lygio elektroninės atpažinties priemonėmis. Pakankamo saugumo užtikrinimo lygmens elektroninės atpažinties priemonėmis turėtų būti kliaujamasi tik tais atvejais, kai suderintos techninės ir veikimo specifikacijos naudojant pakankamo saugumo užtikrinimo lygmens elektroninės atpažinties priemones kartu su kitomis papildomomis tapatybės tikrinimo priemonėmis leis įvykdyti šiame reglamente nustatytus reikalavimus dėl aukšto saugumo užtikrinimo lygio. Tokios papildomos priemonės turėtų būti patikimos ir patogios naudoti naudotojams ir galėtų būti grindžiamos galimybe naudoti nuotolinio prisijungimo procedūras, kvalifikuotus sertifikatus, pagrįstus kvalifikuotais parašais, kvalifikuotu elektroniniu požymių liudijimu arba jų deriniu. Siekiant užtikrinti pakankamą europinių skaitmeninės tapatybės dėklių diegimą, įgyvendinimo aktuose turėtų būti nustatytos suderintos naudotojų prisijungimo naudojant elektroninės atpažinties priemones, įskaitant pakankamo saugumo užtikrinimo lygmens priemones, techninės ir veikimo specifikacijos;

(10b) šio reglamento tikslas – užtikrinti naudotojui visiškai mobilią, saugią ir patogią naudoti europinę skaitmeninės tapatybės dėklę. Kaip pereinamojo laikotarpio priemonė, europinių skaitmeninės tapatybės dėklių, kol bus prieinami sertifikuoti nuo klastojimo apsaugantys sprendimai, pvz., saugūs elementai naudotojų prietaisuose, atveju gali būti kliaujamasi sertifikuotais išoriniais saugiais elementais kriptografinei medžiagai ir kitiems neskelbtiniems duomenims apsaugoti arba nacionaliniais aukšto lygio saugumo užtikrinimo sprendimais, apie kuriuos pranešta, siekiant įrodyti, kad laikomasi atitinkamų reglamento reikalavimų dėl dėklės saugumo užtikrinimo lygio. Pirmiau minėta pereinamojo laikotarpio priemonė turėtų būti taikoma tik tais atvejais, kai reikalingas aukštas saugumo užtikrinimo lygis, pvz., naudotojui prisijungiant prie dėklės ir atliekant tapatumo nustatymo procedūrą prieigai prie paslaugų, kurių atveju reikalingas aukštas saugumo užtikrinimo lygis. Kai tapatumo nustatymas atliekamas prieigai prie paslaugų, kurių atveju reikalingas pakankamas saugumo užtikrinimo lygis, naudoti pirmiau minėtos pereinamojo laikotarpio priemonės europinių skaitmeninės tapatybės dėklių atveju neturėtų būti reikalaujama. Šiuo reglamentu neturėtų būti daromas poveikis nacionalinėms sertifikuoto išorinio saugaus elemento išdavimo ir naudojimo sąlygoms, jei ši pereinamojo laikotarpio priemonė juo kliaujasi;

(11) europinėmis skaitmeninės tapatybės dėklėmis turėtų būti užtikrinta aukščiausio lygio tapatumui nustatyti naudojamų asmens duomenų apsauga ir saugumas, nepriklausomai nuo to, ar tokie duomenys saugomi vietoje, ar naudojant debesijos sprendimus, atsižvelgiant į skirtingų lygių riziką. Biometrinių duomenų tvarkymas kaip tapatumo nustatymo veiksnys siekiant saugiau nustatyti naudotojo tapatumą yra viena iš atpažinties priemonių, suteikianti aukštą patikimumo lygį, visų pirma, kai jie naudojami kartu su kitais tapatumo nustatymo elementais. Kadangi biometriniai duomenys yra unikali asmens savybė, tvarkyti biometrinius duomenis leidžiama tik atsižvelgiant į Reglamento (ES) 2016/679 9 straipsnio 2 dalies išimtis ir reikalaujama taikyti tinkamas apsaugos priemones, atitinkančias riziką, kurią toks tvarkymas gali kelti fizinių asmenų teisėms ir laisvėms;

(11a) europinių skaitmeninės tapatybės dėklių veikimas turėtų būti skaidrus ir sudaryti sąlygas patikrinti, kaip tvarkomi asmens duomenys. Siekiant šio tikslo, valstybės narės skatinamos atskleisti europinių skaitmeninės tapatybės dėklių programinės įrangos komponentų, susijusių su asmens duomenų ir juridinių asmenų duomenų tvarkymu, pirminį kodą. Tokio pirminio kodo atskleidimas leidžia visuomenei, įskaitant naudotojus ir kūrėjus, suprasti jo veikimą. Tai taip pat gali padidinti naudotojų pasitikėjimą dėklės ekosistema ir prisidėti prie dėklių saugumo, nes suteikiama galimybė visiems pranešti apie kodo pažeidžiamumus ir klaidas. Tai skatina tiekėjus pateikti ir palaikyti labai saugų produktą. Be to, kai tinkama, valstybės narės taip pat skatinamos suteikti pirminį kodą pagal atvirosios programinės įrangos licenciją. Atvirosios programinės įrangos licencija suteikia galimybę visuomenei, įskaitant naudotojus ir kūrėjus, iš dalies keisti ir pakartotinai naudoti pirminį kodą;

(12) siekdamos užtikrinti, kad Europos skaitmeninės tapatybės sistema būtų atvira naujovėms, technologiniams pokyčiams ir perspektyvi, valstybės narės turėtų būti skatinamos kartu nustatyti bandomąją aplinką, kurioje būtų saugiai ir prižiūrint išbandomi novatoriški sprendimai, visų pirma siekiant pagerinti funkcionalumą, asmens duomenų apsaugą, sprendimų saugumą ir sąveikumą bei pranešti apie būsimus techninių standartų ir teisinių reikalavimų naujinimus. Ši aplinka turėtų skatinti Europos mažų ir vidutinių įmonių, startuolių ir atskirų novatorių bei tyrėjų įtrauktį;

(13) Reglamentu (ES) Nr. 2019/1157[7] stiprinamas asmens tapatybės kortelių saugumas iki 2021 m. rugpjūčio mėn. įdiegus geresnes apsaugos funkcijas. Valstybės narės turėtų apsvarstyti pranešimo joms galimybę taikant elektroninės atpažinties schemas, siekdamos išplėsti tarpvalstybinį elektroninės atpažinties priemonių prieinamumą;

(14) reikėtų supaprastinti ir paspartinti pranešimo apie elektroninės atpažinties schemas procesą, kad būtų remiamas patogių, patikimų, saugių ir novatoriškų tapatumo nustatymo ir atpažinties sprendimų prieinamumas ir, prireikus, skatinti privačius tapatybės teikėjus valstybės narės institucijoms siūlyti elektroninės atpažinties schemas, kad šios praneštų apie jas kaip apie nacionalines elektroninės atpažinties schemas pagal Reglamento (ES) Nr. 910/2014 nuostatas;

(15) supaprastinus esamą pranešimų ir tarpusavio vertinimo tvarką, bus užkirstas kelias įvairialypiams požiūriams vertinant įvairias elektroninės atpažinties schemas, apie kurias pranešta, ir bus lengviau kuriamas pasitikėjimas tarp valstybių narių. Nauji, supaprastinti mechanizmai turėtų paskatinti valstybes nares bendradarbiauti elektroninės atpažinties schemų, apie kurias jos pranešė, saugumo ir sąveikumo srityse;

(16) valstybės narės turėtų gauti naudos iš naujų, lanksčių priemonių, skirtų atitikčiai šio reglamento ir atitinkamų įgyvendinimo aktų reikalavimams užtikrinti. Šiuo reglamentu valstybėms narėms turėtų būti sudarytos sąlygos naudotis akredituotų atitikties vertinimo įstaigų parengtomis ataskaitomis ir vertinimais, kaip numatyta sertifikavimo schemose, kurios turi būti nustatytos Sąjungos lygmeniu pagal Reglamentą (ES) 2019/881, kad būtų pagrįsti jų reikalavimai suderinti schemas ar jų dalis su reglamente dėl elektroninės atpažinties schemų, apie kurias pranešta, sąveikumo ir saugumo išdėstytais reikalavimais;

---

[7] 2019 m. birželio 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/1157 dėl Sąjungos piliečių tapatybės kortelių ir Sąjungos piliečiams bei jų šeimos nariams, kurie naudojasi laisvo judėjimo teise, išduodamų teisę gyventi šalyje patvirtinančių dokumentų saugumo didinimo (OL L 188, 2019 7 12, p. 67).

(17a) valstybių narių išduotų arba europinės skaitmeninės tapatybės dėklės sukurtų unikalių ir nekintamų identifikatorių naudojimas kartu su asmens tapatybės duomenų naudojimu yra labai svarbūs siekiant užtikrinti, kad būtų galima patikrinti naudotojo tapatybę, visų pirma viešajame sektoriuje ir kai tai pavesta pagal nacionalinę ar Sąjungos teisę. Šiuo reglamentu turėtų būti užtikrinta, kad europinė skaitmeninės tapatybės dėklė galėtų būti mechanizmas, kuris leistų atlikti įrašų atpažinties procesą, be kita ko, naudojant kvalifikuotus elektroninius požymių liudijimus, ir sudarytų sąlygas į asmens tapatybės duomenų rinkinį įtraukti unikalius ir nekintamus identifikatorius. Unikalus ir nekintamas identifikatorius gali būti sudarytas iš vieno arba kelių identifikacinių duomenų, kurie gali būti konkretūs sektoriui, jei pagal juos galima tiksliai identifikuoti naudotoją visoje Sąjungoje. Europinė skaitmeninės tapatybės dėklė taip pat turėtų būti mechanizmas, leidžiantis naudoti pasikliaujančiosios šalies specifinius identifikatorius tais atvejais, kai pagal nacionalinę arba Sąjungos teisę reikalaujama naudoti unikalų ir nekintamą identifikatorių. Visais atvejais mechanizmas, skirtas palengvinti įrašų atpažintį ir unikalių ir nekintamų identifikatorių naudojimą, turėtų užtikrinti, kad naudotojas pagal šį reglamentą ir taikytiną Sąjungos teisę, visų pirma Reglamentą (ES) 2016/679, būtų apsaugotas nuo netinkamo asmens duomenų naudojimo, be kita ko, nuo profiliavimo ir sekimo rizikos, susijusios su europinės skaitmeninės tapatybės dėklės naudojimu;

(17aaa) labai svarbu atsižvelgti į naudotojų poreikius ir taip padidinti europinių skaitmeninės tapatybės dėklių paklausą. Turėtų būti prieinami prasmingo naudojimo atvejai ir internetinės paslaugos, kurias teikiant kliaujamasi europinėmis skaitmeninės tapatybės dėklėmis. Naudotojų patogumui ir siekiant užtikrinti tarpvalstybinį tokių paslaugų prieinamumą, svarbu imtis veiksmų, kad būtų sudarytos palankesnės sąlygos panašiam požiūriui į internetinių paslaugų kūrimą, plėtojimą ir įgyvendinimą visose valstybėse narėse. Naudinga priemone šiam tikslui pasiekti galėtų būti neprivalomos gairės, kaip kurti, plėtoti ir įgyvendinti internetines paslaugas, kurias teikiant kliaujamasi europinėmis skaitmeninės tapatybės dėklėmis. Šios gairės turėtų būti parengtos tinkamai atsižvelgiant į Sąjungos sąveikumo sistemą. Valstybėms narėms turėtų tekti pagrindinis vaidmuo jas priimant;

(18) laikantis Direktyvos (ES) 2019/882[8] nuostatų, neįgalieji turėtų turėti galimybę vienodomis sąlygomis kaip ir kiti naudotojai naudotis europinėmis skaitmeninės tapatybės dėklėmis, patikimumo užtikrinimo paslaugomis ir galutiniams vartotojams skirtais produktais, naudojamais teikiant tas paslaugas;

(19) šiuo reglamentu neturėtų būti reglamentuojami aspektai, susiję su sutarčių sudarymu arba kitų teisinių pareigų nustatymu ir šių sutarčių bei pareigų galiojimu, kai nacionalinės arba Sąjungos teisės aktais yra nustatyti reikalavimai dėl formos. Be to, juo nedaromas poveikis nacionalinės formos reikalavimams, susijusiems su viešaisiais registrais, visų pirma, komerciniais ir žemės registrais;

(20) patikimumo užtikrinimo paslaugų teikimas ir naudojimas tampa vis svarbesni tarptautinės prekybos ir bendradarbiavimo srityse. ES tarptautiniai partneriai, įkvėpti Reglamento (ES) Nr. 910/2014, nustatinėja patikimumo užtikrinimo sistemas. Dėl to siekiant palengvinti tokių paslaugų ir jų teikėjų pripažinimą, įgyvendinimo teisės aktuose galima nustatyti sąlygas, kuriomis trečiųjų šalių patikimumo užtikrinimo sistemas būtų galima laikyti lygiavertėmis kvalifikuotų patikimumo užtikrinimo paslaugų ir teikėjų patikimumo užtikrinimo sistemai pagal šį reglamentą – tokios sąlygos papildytų patikimumo užtikrinimo paslaugų ir Sąjungoje ir trečiosiose šalyse įsteigtų teikėjų tarpusavio pripažinimą pagal Sutarties 218 straipsnį; Šiame reglamente nustatant sąlygas, kuriomis trečiųjų valstybių patikimumo užtikrinimo sistemos galėtų būti laikomos lygiavertėmis kvalifikuotų patikimumo užtikrinimo paslaugų ir teikėjų patikimumo užtikrinimo sistemai, taip pat turėtų būti užtikrinta atitiktis atitinkamoms Direktyvos XXXX/XXXX (TIS 2 direktyvos) ir Reglamento (ES) 2016/679 nuostatoms, taip pat turėtų būti užtikrintas patikimų sąrašų kaip esminių pasitikėjimo stiprinimo elementų naudojimas;

---

[8] 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos direktyva (ES) 2019/882 dėl gaminių ir paslaugų prieinamumo reikalavimų (OL L 151, 2019 6 7, p. 70).

(21) šis reglamentas turėtų būti grindžiamas Sąjungos teisės aktais, kuriais skaitmeniniame sektoriuje užtikrinamos konkurencingos ir sąžiningos rinkos. Visų pirma jis pagrįstas Reglamentu (ES) 2022/1925, kuriame nustatytos taisyklės pagrindinių paslaugų platformų teikėjams, kurie paskirti prieigos valdytojais, ir, be kita ko, prieigos valdytojams draudžiama reikalauti, kad verslo klientai, siūlydami savo paslaugas to prieigos valdytojo pagrindinių paslaugų platformoje, naudotųsi prieigos valdytojo atpažinties paslauga, ją siūlytų ar su ja sąveikautų. Reglamento 2022/1925 6 straipsnio 7 dalyje reikalaujama, kad prieigos valdytojai suteiktų verslo klientams ir pagalbinių paslaugų teikėjams prieigą prie tos pačios operacinės sistemos, aparatinės įrangos ar programinės įrangos funkcijų, kurios prieinamos prieigos valdytojui, kai jis teikia pagalbines paslaugas, ar kuriomis jis naudojasi teikdamas tas paslaugas, ir užtikrintų jų sąveikumą. Pagal Skaitmeninių rinkų akto 2 straipsnio 15 punktą atpažinties paslaugos yra viena iš pagalbinių paslaugų rūšių. Dėl to pagalbinių paslaugų verslo klientai ir teikėjai turėtų turėti galimybę naudotis tokiomis aparatinės įrangos ar programinės įrangos funkcijomis, kaip išmaniuosiuose telefonuose įdiegti saugūs elementai, ir su jomis sąveikauti per europines skaitmeninės tapatybės dėkles ar elektroninės atpažinties priemones, apie kurias pranešė valstybės narės;

(22) siekiant supaprastinti patikimumo užtikrinimo paslaugų teikėjams taikomus kibernetinio saugumo įpareigojimus ir suteikti šiems teikėjams bei jų atitinkamoms kompetentingoms institucijoms galimybę pasinaudoti pagal Direktyvą XXXX/XXXX (TIS2 direktyvą) nustatyta teisine sistema, teikiant patikimumo užtikrinimo paslaugas turi būti taikomos tinkamos techninės ir organizacinės priemonės laikantis Direktyvos XXXX/XXXX (TIS2 direktyvos) nuostatų, pvz., su sistemos triktimi, žmogiška klaida, piktavališkais veiksmais ar gamtiniais reiškiniais susijusios priemonės siekiant valdyti tinklų ir informacinėms sistemoms, kurias tie teikėjai naudoja teikdami savo paslaugas, keliamą riziką ir siekiant pranešti apie reikšmingus incidentus bei kibernetines grėsmes pagal Direktyvą XXXX/XXXX (TIS2 direktyvą). Atsižvelgdami į pranešimus apie incidentus, patikimumo užtikrinimo paslaugų teikėjai turėtų pranešti apie bet kokius incidentus, darančius reikšmingą poveikį jų paslaugų teikimui, įskaitant dėl vagystės ar įtaisų praradimo, tinklo kabelių pažeidimų kilusius incidentus ar incidentus, kilusius asmenų tapatybės nustatymo aplinkybėmis. Kibernetinio saugumo rizikos valdymo reikalavimus ir įpareigojimus teikti pranešimus pagal Direktyvą XXXXXX [TIS2] reikėtų svarstyti kartu su patikimumo užtikrinimo paslaugų teikėjams keliamais reikalavimais pagal šį reglamentą. Kai taikoma, pagal Direktyvą XXXX/XXXX (TIS2 direktyvą) paskirtosios kompetentingos institucijos turėtų ir toliau taikyti nustatytą nacionalinę praktiką ar gaires dėl saugumo ir pranešimų teikimo reikalavimų įgyvendinimo bei tokių reikalavimų laikymosi priežiūros pagal Reglamentą (ES) Nr. 910/2014. Bet kokie su šiuo reglamentu susiję reikalavimai nedaro poveikio įpareigojimui pranešti apie asmens duomenų apsaugos pažeidimus pagal Reglamentą (ES) 2016/679;

(23) reikėtų deramai atsižvelgti į būtinybę užtikrinti veiksmingą TIS ir eIDAS institucijų bendradarbiavimą. Tais atvejais, kai priežiūros institucija pagal šį reglamentą skiriasi nuo kompetentingų institucijų, paskirtųjų pagal Direktyvą XXXX/XXXX [NIS2], tokios institucijos turėtų glaudžiai bendradarbiauti, laiku keisdamosi aktualia informacija, kad užtikrintų veiksmingą patikimumo užtikrinimo paslaugų teikėjų priežiūrą ir jų atitiktį šiame reglamente ir Direktyvoje XXXX/XXXX [NIS2] nustatytiems reikalavimams. Visų pirma priežiūros institucijos pagal šį reglamentą turėtų turėti teisę prašyti, kad Direktyvoje XXXXX/XXXX [TIS2] nurodyta kompetentinga institucija teiktų aktualią informaciją, reikalingą suteikti kvalifikuotą statusą ir atlikti priežiūros veiksmus, siekiant patikrinti patikimumo užtikrinimo paslaugų teikėjų atitiktį atitinkamiems reikalavimams pagal TIS 2 arba reikalauti, kad jie pašalintų neatitikimus;

(24) būtina numatyti teisinį pagrindą, kad būtų sudaromos palankesnės sąlygos tarpvalstybiniam esamų nacionalinių teisės sistemų, susijusių su elektroninio registruoto pristatymo paslaugomis, pripažinimui. Be to, ta sistema galėtų atverti naujas rinkos galimybes Sąjungos patikimumo užtikrinimo paslaugų teikėjams siūlyti naujas Europos masto elektroninio registruoto pristatymo paslaugas. Siekiant užtikrinti, kad duomenys naudojantis kvalifikuota elektroninio registruoto pristatymo paslauga būtų teikiami teisingam adresatui, teikiant kvalifikuotas elektroninio registruoto pristatymo paslaugas turėtų būti visiškai užtikrinama, kad būtų identifikuotas adresatas, o siuntėjui identifikuoti pakaktų aukšto patikimumo lygio. Valstybės narės turėtų skatinti kvalifikuotų elektroninio registruoto pristatymo paslaugų teikėjus užtikrinti, kad jų paslaugos būtų sąveikios su kitų kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų teikiamomis kvalifikuotomis elektroninio registruoto pristatymo paslaugomis, kad būtų galima lengvai perduoti elektroninius registruotus duomenis tarp dviejų ar daugiau kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų ir skatinti sąžiningą praktiką vidaus rinkoje;

(25) daugeliu atvejų piliečiai ir kiti gyventojai negali skaitmeniniu būdu, tarpvalstybiniu mastu saugiai keistis su jų tapatybe susijusia informacija, pvz., adresais, amžiumi ir profesinėmis kvalifikacijomis, vairuotojo pažymėjimais ir kitais leidimais bei mokėjimo duomenimis užtikrinant aukštą duomenų apsaugos lygį;

(26) turėtų būti suteikta galimybė išleisti ir tvarkyti patikimus skaitmeninius požymius ir prisidėti prie administracinės naštos mažinimo, įgalinant piliečius ir kitus gyventojus jais naudotis atliekant savo privačiąsias ir viešąsias operacijas. Piliečiai ir kiti gyventojai turėtų turėti galimybę, pavyzdžiui, įrodyti, kad jie turi vienos valstybės narės institucijos išduotą galiojantį vairuotojo pažymėjimą, kurį gali patikrinti ir juo kliautis atitinkamos kitų valstybių narių institucijos, pasikliauti savo socialinio draudimo kredencialais ar būsimais skaitmeniniais kelionės dokumentais tarpvalstybiniu mastu;

(27) bet kuris patikrintus požymius, tokius kaip diplomai, licencijos, gimimo liudijimai, renkantis, kuriantis ir išduodantis subjektas turėtų turėti galimybę tapti elektroninių požymių liudijimų teikėju. Pasikliaujančiosios šalys turėtų naudotis elektroniniais požymių liudijimais kaip lygiaverčiais popierinio formato liudijimams. Dėl to negalima atsisakyti pripažinti elektroninio požymių liudijimo teisinės galios tik dėl to, kad parašas yra elektroninis arba kad jis neatitinka kvalifikuoto elektroninio požymių liudijimo reikalavimų. Tuo tikslu reikėtų nustatyti bendruosius reikalavimus siekiant užtikrinti, kad kvalifikuoto elektroninio požymių liudijimo teisinė galia prilygtų popierinių teisėtai išduotų liudijimų teisinei galiai. Tačiau tie reikalavimai turėtų būti taikomi nepažeidžiant Sąjungos ir nacionalinės teisės aktų, kuriais nustatomi papildomi konkretiems sektoriams taikomi reikalavimai dėl formos ir teisinės galios ir visų pirma tarpvalstybinio kvalifikuotų elektroninių požymių liudijimų pripažinimo, kai taikoma;

(28) siekiant plataus europinių skaitmeninės tapatybės dėklių prieinamumo ir tinkamumo naudoti, būtina, kad jas pripažintų privačiųjų paslaugų teikėjai. Privačiosios pasikliaujančiosios šalys, teikiančios paslaugas transporto, energetikos, bankininkystės srityse, finansines paslaugas, socialinės apsaugos, sveikatos, geriamojo vandens, pašto paslaugas, skaitmeninės infrastruktūros, švietimo ar telekomunikacijų paslaugas, turėtų sutikti su europinių skaitmeninės tapatybės dėklių naudojimu teikiant paslaugas, kai pagal nacionalinę ar Sąjungos teisę arba pagal sudarytas sutartis būtina užtikrinti saugesnį naudotojo tapatumo nustatymą. Siekiant palengvinti europinės skaitmeninės tapatybės dėklės naudojimą ir pripažinimą, reikėtų atsižvelgti į plačiai pripažintus pramonės standartus ir specifikacijas. Kai labai didelėse interneto platformose, kaip apibrėžta reglamento 25.1 straipsnyje [nuoroda į SPA reglamentą], reikalaujama nustatyti naudotojų tapatumą, kad jie galėtų naudotis internetinėmis paslaugomis, tokios platformos turėtų būti įgaliotos pritarti europinių skaitmeninės tapatybės dėklių naudojimui naudotojui savanoriškai prašant. Naudotojams neturėtų būti taikomas įpareigojimas naudoti dėkles, kad galėtų naudotis privačiosiomis paslaugomis, bet jiems pageidaujant tai daryti, didelės interneto platformos šiuo tikslu turėtų pripažinti europinę skaitmeninės tapatybės dėklę, laikydamosi duomenų kiekio mažinimo principo. Atsižvelgiant į labai didelių interneto platformų svarbą dėl jų aprėpties, visų pirma išreiškiamos paslaugos gavėjų ir ekonominių operacijų skaičiumi, būtina padidinti naudotojų apsaugą nuo sukčiavimo ir užtikrinti aukšto lygio duomenų apsaugą. Sąjungos lygmeniu reikėtų parengti savireguliavimo elgesio kodeksus (toliau – elgesio kodeksai), siekiant prisidėti prie elektroninės atpažinties priemonių plataus prieinamumo ir tinkamumo naudoti, įskaitant pagal šio reglamento taikymo sritį naudojamas europines skaitmeninės tapatybės dėkles. Elgesio kodeksais turėtų būti palengvintas platus elektroninės atpažinties priemonių priėmimas, įskaitant europines skaitmeninės tapatybės dėkles, tų paslaugų teikėjų, kurie nėra laikomi labai didelėmis platformomis ir kurie pasikliauja trečiųjų šalių elektroninės atpažinties paslaugomis naudotojų tapatumui nustatyti, atveju. Jie turėtų būti parengti per 12 mėnesių nuo šio reglamento priėmimo dienos. Komisija praėjus 24 mėnesiams nuo europinių skaitmeninės tapatybės dėklių įdiegimo turėtų įvertinti šių nuostatų veiksmingumą dėl prieinamumo naudotojui ir jų tinkamumo naudoti;

(29) pasirinktinis atskleidimas – tai koncepcija, kuria duomenų savininkui suteikiama teisė atskleisti tik tam tikras didesnio duomenų rinkinio dalis, kad gaunantis subjektas gautų tik reikiamą informaciją, pvz., kad naudotojas atskleistų tik tuos duomenis pasikliaujančiajai šaliai, kurie yra būtini paslaugai, kurios prašo naudotojas, teikti. europine skaitmeninės tapatybės dėkle turėtų būti suteikta techninė galimybė pasirinkti, kuriuos požymius atskleisti pasikliaujančiosioms šalims. Tokie pasirinktinai atskleidžiami požymiai, įskaitant atvejus, kai pradžioje jie buvo kelių atskirų elektroninių liudijimų dalys, vėliau gali būti sujungiami ir pateikiami pasikliaujančiosioms šalims. Ši funkcija turėtų tapti pagrindine konstrukcine funkcija, kuria bus gerinamas patogumas ir stiprinama asmens duomenų apsauga, įskaitant duomenų kiekio mažinimą;

(30) kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų teikiamus požymius, įtraukiamus į kvalifikuotus požymių liudijimus, reikėtų patikrinti pagal autentiškus šaltinius tiesiogiai pagal kvalifikuotą patikimumo užtikrinimo paslaugų teikėją arba per paskirtuosius tarpininkus, kurie pripažįstami nacionaliniu lygmeniu, remiantis nacionaline ar Sąjungos teise, siekiant atpažinties ar požymių liudijimų paslaugų teikėjams ir pasikliaujančiosioms šalims saugiai keistis patikrintais požymiais. Valstybės narės turėtų nacionaliniu lygmeniu nustatyti tinkamus mechanizmus, kuriais būtų užtikrinta, kad kvalifikuotus elektroninius požymių liudijimus išduodantys kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai, remdamiesi asmens, kuriam išduodamas liudijimas, sutikimu, galėtų patikrinti požymių autentiškumą, kliaudamiesi autentiškais šaltiniais. Tinkami mechanizmai gali apimti naudojimąsi konkrečiais tarpininkais arba techninius sprendimus, atitinkančius nacionalinės teisės aktus, kuriais suteikiama prieiga prie autentiškų šaltinių. Užtikrinus galimybę naudotis mechanizmu, kuriuo būtų sudarytos sąlygos patikrinti požymius pagal autentiškus šaltinius, kvalifikuotiems elektroninių požymių liudijimų teikėjams turėtų būti lengviau laikytis šiuo reglamentu nustatytų pareigų. VI priede pateiktas požymių, kurių atžvilgiu valstybės narės turėtų užtikrinti, kad būtų imtasi priemonių, kad kvalifikuoti elektroninių požymių liudijimų teikėjai galėtų naudotojo prašymu elektroniniu būdu patikrinti jų autentiškumą pagal atitinkamą autentišką šaltinį, kategorijų sąrašas. Dėl konkrečių šioms kategorijoms priskiriamų požymių turėtų būti susitarta tarp valstybių narių;

(31) saugia elektronine atpažintimi ir teikiant požymių liudijimus finansų paslaugų sektoriuje turėtų būti užtikrintas papildomas lankstumas ir sprendimai, kad būtų galima nustatyti klientų tapatybę ir keistis specialiaisiais požymiais siekiant vykdyti, pavyzdžiui, vartotojų išsamaus patikrinimo reikalavimus pagal Kovos su pinigų plovimu reglamentą [priėmus pasiūlymą įtraukti nuorodą], investuotojų apsaugos teisės aktuose nustatytus tinkamumo reikalavimus, ar siekiant įvykdyti saugesnio klientų tapatumo nustatymo, susijusio su elektronine atpažintimi, reikalavimus prisijungiant prie sąskaitos ir inicijuojant operacijas mokėjimo paslaugų srityje;

(31a) siekdama užtikrinti sertifikavimo praktikos nuoseklumą visoje ES, Komisija turėtų paskelbti kvalifikuotų elektroninio parašo kūrimo įtaisų ir kvalifikuotų elektroninio spaudo kūrimo įtaisų sertifikavimo ir pakartotinio sertifikavimo gaires, įskaitant jų galiojimą ir laiko apribojimus. Šiuo reglamentu valstybėms narėms neužkertamas kelias leisti viešosioms ar privačioms įstaigoms, turinčioms sertifikuotus kvalifikuotus elektroninio parašo kūrimo įtaisus, laikinai pratęsti sertifikato galiojimą, kai to paties įtaiso pakartotinis sertifikavimas per teisiškai nustatytą laikotarpį negalėjo būti atliktas dėl kitos priežasties nei pažeidimas ar saugumo incidentas, ir nedarant poveikio taikytinai sertifikavimo praktikai;

(32) interneto svetainių tapatumo nustatymo paslaugos suteikia naudotojams aukšto lygio patikinimą, kad interneto svetainė, nepriklausomai nuo to, kokioje platformoje ji pateikiama, priklauso tikram ir teisėtam subjektui. Tos paslaugos padeda didinti pasitikėjimą verslo vykdymu internete ir mažinti sukčiavimo internete atvejų skaičių. Interneto svetainėms neturėtų būti privaloma naudoti interneto svetainių tapatumo nustatymo paslaugos. Vis dėlto norint, kad interneto svetainės tapatumo nustatymas taptų pasitikėjimo didinimo priemone, kuri pagerintų vartotojo patirtį ir toliau skatintų vidaus rinkos augimą, šiame reglamente turėtų būti nustatytos minimalios saugumo ir atsakomybės pareigos interneto svetainių tapatumo nustatymo paslaugų teikėjams ir jų paslaugoms. Todėl pagal Reglamentą (ES) Nr. 910/2014 interneto naršyklių teikėjai turėtų užtikrinti suderinamumą ir sąveikumą su kvalifikuotais interneto svetainių tapatumo nustatymo sertifikatais. Jie turėtų pripažinti kvalifikuotus interneto svetainių tapatumo nustatymo sertifikatus ir leisti, remiantis pagal šį reglamentą nustatytomis specifikacijomis, naršyklės aplinkoje rodyti sertifikuotus tapatybės duomenis galutiniam naudotojui. Kvalifikuoto interneto svetainės tapatumo nustatymo sertifikato pripažinimas kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo išduotu kvalifikuotu sertifikatu turėtų užtikrinti, kad sertifikate pateiktų tapatybės duomenų autentiškumą būtų galima patvirtinti ir patikrinti pagal šį reglamentą. Tai neturėtų daryti poveikio interneto naršyklių teikėjų galimybei ištaisyti svarbius reikalavimų nesilaikymo atvejus, susijusius su saugumo pažeidimu ir atskirų sertifikatų vientisumo pažeidimu, taip prisidedant prie galutinių naudotojų saugumo internete. Siekdamos ir toliau apsaugoti piliečius ir skatinti naudojimąsi kvalifikuotais interneto svetainių tapatumo nustatymo sertifikatais, valstybių narių valdžios institucijos turėtų apsvarstyti galimybę juos įdiegti į savo interneto svetaines;

(33) daugelis valstybių narių priėmė nacionalinius reikalavimus dėl saugaus ir patikimo skaitmeninio archyvavimo paslaugų, siekdamos sudaryti elektroninių duomenų ir susijusių patikimumo užtikrinimo paslaugų ilgalaikio išsaugojimo galimybę. Siekiant užtikrinti teisinį tikrumą, pasitikėjimą ir suderinimą visose valstybėse narėse, turėtų būti sukurta kvalifikuotų elektroninio archyvavimo paslaugų teisinė sistema, grindžiama kitų šiame reglamente nustatytų patikimumo užtikrinimo paslaugų sistema. Ši sistema turėtų suteikti patikimumo užtikrinimo paslaugų teikėjams ir naudotojams veiksmingą priemonių rinkinį, apimantį funkcinius elektroninio archyvavimo paslaugos reikalavimus, taip pat turėti aiškias teisines pasekmes, kai naudojamasi kvalifikuota elektroninio archyvavimo paslauga. Šios nuostatos turėtų būti taikomos elektroniniu būdu parengtiems dokumentams ir popieriniams dokumentams, kurie buvo nuskenuoti ir suskaitmeninti. Prireikus pagal šias nuostatas turėtų būti leidžiama saugomus elektroninius duomenis perkelti į įvairias laikmenas arba formatus, kad jų patvarumas ir įskaitomumas būtų ilgesnis už technologinio galiojimo laikotarpį, kartu kuo labiau sumažinant praradimo ir pakeitimo galimybę. Kai skaitmeninio archyvavimo paslaugai pateiktuose elektroniniuose duomenyse yra vienas ar daugiau kvalifikuotų elektroninių parašų arba kvalifikuotų elektroninių spaudų, teikiant paslaugą turėtų būti naudojamos procedūros ir technologijos, kuriomis būtų galima padidinti jų patikimumą tokių duomenų saugojimo laikotarpiu, galbūt kliaujantis kitų šiuo reglamentu nustatytų kvalifikuotų elektroninių patikimumo užtikrinimo paslaugų naudojimu. Išsaugojimo įrodymams kurti, kai naudojami elektroniniai parašai, elektroniniai spaudai arba elektroninės laiko žymos, turėtų būti naudojamos kvalifikuotos elektroninės patikimumo užtikrinimo paslaugos. Tiek, kiek elektroninio archyvavimo paslaugos šiuo reglamentu nėra suderintos, valstybės narės, laikydamosi Sąjungos teisės, gali toliau taikyti arba priimti nacionalines nuostatas, susijusias su tomis paslaugomis, pavyzdžiui, konkrečias nuostatas, kuriomis leidžiama taikyti tam tikras leidžiančias nukrypti nuostatas paslaugų, kurios yra integruotos į organizaciją ir naudojamos tik šios organizacijos „vidaus archyvų“ reikmėms, atveju. Šiame reglamente neturėtų būti daromas skirtumas tarp elektroniniu būdu parengtų dokumentų ir suskaitmenintų fizinių dokumentų;

(33a) nacionaliniai archyvai ir atminties institucijos, kaip organizacijos, kurių paskirtis – išsaugoti viešojo intereso dokumentinį paveldą, paprastai yra įgaliotos vykdyti savo veiklą pagal nacionalinę teisę ir nebūtinai teikia patikimumo užtikrinimo paslaugas, kaip tai suprantama šiame reglamente. Tiek, kiek šios įstaigos neteikia tokių paslaugų, šis reglamentas nedaro poveikio jų veiklai;

(34) elektroniniai registrai yra elektroninių duomenų įrašų seka, kuriais užtikrinamas jų vientisumas ir jų chronologinės tvarkos tikslumas. Elektroninių registrų tikslas – sukurti chronologinę duomenų įrašų seką, kad skaitmeninis turtas nebūtų kopijuojamas ir parduodamas keliems gavėjams. Elektroniniai registrai gali būti naudojami, pavyzdžiui, skaitmeniniams įrašams apie nuosavybę pasaulinėje prekyboje, tiekimo grandinės finansavimui, intelektinės nuosavybės teisių arba biržinių prekių, pavyzdžiui, elektros energijos, skaitmeninimui. Kartu su kitomis technologijomis jie gali prisidėti prie sprendimų dėl veiksmingesnių ir transformatyvių viešųjų paslaugų, tokių kaip e. balsavimas, muitinių tarpvalstybinis bendradarbiavimas, tarpvalstybinis akademinių institucijų bendradarbiavimas arba nekilnojamojo turto nuosavybės registravimas decentralizuotuose žemės registruose. Kvalifikuoti elektroniniai registrai sukuria teisinę prezumpciją dėl unikalios ir tikslios nuoseklios chronologinės registro duomenų įrašų tvarkos ir vientisumo. Dėl specifinių elektroninių registrų požymių, t. y. nuoseklios chronologinės duomenų įrašų tvarkos, daromas skirtumas tarp elektroninių registrų ir kitų patikimumo užtikrinimo paslaugų, pavyzdžiui, elektroninių laiko žymų ir elektroninio registruoto pristatymo paslaugų. T. y. nei skaitmeninių dokumentų laiko žymėjimas, nei jų perdavimas naudojantis elektroninio registruoto pristatymo paslaugomis, jei nebus imtasi papildomų techninių ar organizacinių priemonių, negalėtų pakankamai užkirsti kelio to paties skaitmeninio turto kopijavimui ir pardavimui skirtingoms šalims daugiau nei vieną kartą. Elektroninio registro sukūrimo ir atnaujinimo procesas priklauso nuo naudojamo (centralizuoto ar paskirstytojo) registro tipo;

(35) siekiant užkirsti kelią vidaus rinkos susiskaidymui turėtų būti nustatyta europinė teisinė sistema, sudaranti sąlygas pripažinti patikimumo užtikrinimo paslaugas, skirtas registruoti duomenis kvalifikuotuose elektroniniuose registruose, tarpvalstybiniu mastu. Elektroninių registrų patikimumo užtikrinimo paslaugų teikėjai turėtų būti įgalioti užtikrinti nuoseklų duomenų registravimą registre. Šis reglamentas taikomas neatsižvelgiant į teisines pareigas, kurių elektroninių registrų naudotojams gali reikėti laikytis pagal Sąjungos ir nacionalinę teisę. Pavyzdžiui, tokiais atvejais, kai tvarkomi asmens duomenys, turėtų būti laikomasi Reglamento (ES) 2016/679. Su kriptoturtu susiję naudojimo atvejai turėtų būti suderinami su visomis taikytinomis finansinėmis taisyklėmis, įskaitant, pavyzdžiui, Finansinių priemonių rinkų direktyvą[9], Mokėjimo paslaugų direktyvą[10], Elektroninių pinigų direktyvą[11], taip pat su galimais būsimais teisės aktais dėl kriptoturto rinkų ir su kovos su pinigų plovimu taisyklėmis, kurios galėtų būti įtrauktos į Lėšų pervedimo reglamentą[12] ir kuriomis galėtų būti reikalaujama, kad kriptoturto paslaugų teikėjai patikrintų elektroninių registrų naudotojų tapatybę, kad būtų laikomasi tarptautinių kovos su pinigų plovimu standartų.

---

9 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos direktyva 2014/65/ES dėl finansinių priemonių rinkų, kuria iš dalies keičiamos Direktyva 2002/92/EB ir Direktyva 2011/61/ES (OL L 173, 2014 6 12, p. 349–496).

10 2015 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva (ES) 2015/2366 dėl mokėjimo paslaugų vidaus rinkoje, kuria iš dalies keičiamos direktyvos 2002/65/EB, 2009/110/EB ir 2013/36/ES bei Reglamentas (ES) Nr. 1093/2010 ir panaikinama Direktyva 2007/64/EB (OL L 337, 2015 12 23, p. 35–127).

11 2009 m. rugsėjo 16 d. Europos Parlamento ir Tarybos direktyva 2009/110/EB dėl elektroninių pinigų įstaigų steigimosi, veiklos ir riziką ribojančios priežiūros, iš dalies keičianti Direktyvas 2005/60/EB ir 2006/48/EB ir panaikinanti Direktyvą 2000/46/EB (OL L 267, 2009 10 10, p. 7–17).

12 Žr. 2021 m. liepos 20 d. Komisijos pasiūlymą nauja redakcija išdėstyti Europos Parlamento ir Tarybos reglamentą (ES) 2015/847 dėl informacijos, teikiamos pervedant lėšas, COM/2021/422 *final*.

(36) siekiant išvengti susiskaidymo ir kliūčių dėl besiskiriančių standartų ir techninių apribojimų ir užtikrinti suderintą procesą, kad būsimos Europos skaitmeninės tapatybės sistemos įgyvendinimui nekiltų pavojus, būtinas glaudaus ir struktūruoto Komisijos, valstybių narių ir privačiojo sektoriaus bendradarbiavimo procesas. Siekdamos šio tikslo valstybės narės turėtų bendradarbiauti vadovaudamosi Komisijos rekomendacijoje XXX/XXXX [Suderinto požiūrio į Europos skaitmeninės tapatybės sistemą priemonių rinkinys][13] nustatyta sistema, kad nustatytų Europos skaitmeninės tapatybės sistemai skirtą priemonių rinkinį. Priemonių rinkinys turėtų apimti išsamią techninę architektūrą ir pavyzdinę sistemą, bendrų standartų ir techninių sąlygų rinkinį bei gairių ir geriausios praktikos aprašymų rinkinį, kuriuose būtų aptarti bent jau visi europinių skaitmeninės tapatybės dėklių funkcionalumo ir sąveikumo aspektai, įskaitant e. parašus, ir kvalifikuotų patikimumo užtikrinimo paslaugų aspektai, susiję su požymių liudijimais, kaip nustatyta šiame reglamente. Į tai atsižvelgdamos valstybės narės taip pat turėtų susitarti dėl bendrų europinių skaitmeninės tapatybės dėklių verslo modelio ir mokesčių struktūros elementų, kad visų pirma mažoms ir vidutinėms įmonėms būtų lengviau jas diegti tarpvalstybiniu mastu. Priemonių rinkinio turinys turėtų keistis priklausomai nuo Europos skaitmeninės tapatybės sistemos diskusijos ir priėmimo proceso rezultato ir jį atspindėti;

36a) valstybės narės turėtų nustatyti taisykles dėl sankcijų už pažeidimus, pavyzdžiui, tiesioginę ar netiesioginę praktiką, dėl kurios painiojamos nekvalifikuotos ir kvalifikuotos patikimumo užtikrinimo paslaugos arba nekvalifikuoti patikimumo užtikrinimo paslaugų teikėjai piktnaudžiauja ES patikimumo ženklo naudojimu. ES patikimumo ženklas neturėtų būti naudojamas tokiomis sąlygomis, kurios tiesiogiai ar netiesiogiai leistų manyti, kad bet kokios šio paslaugų teikėjo siūlomos nekvalifikuotos patikimumo užtikrinimo paslaugos yra kvalifikuotos;

---

13 [Priėmus įterpti nuorodą].

(36b) šiuo reglamentu turėtų būti užtikrintas suderintas kvalifikuotų patikimumo užtikrinimo paslaugų kokybės, patikimumo ir saugumo lygis, neatsižvelgiant į veiklos vykdymo vietą. Todėl kvalifikuotam patikimumo užtikrinimo paslaugų teikėjui turėtų būti leidžiama vykdyti savo veiklą, susijusią su kvalifikuotos patikimumo užtikrinimo paslaugos teikimu už Sąjungos ribų, naudojantis užsakomosiomis paslaugomis, jei jis pateiktų garantijas užtikrindamas, kad priežiūros veiklos ir audito vykdymas galėtų būti užtikrinamas taip, tarsi ši veikla vykdoma Sąjungoje. Kai negalima visiškai užtikrinti, kad bus laikomasi reglamento, priežiūros įstaigos turėtų turėti galimybę priimti proporcingas ir pagrįstas priemones, įskaitant teikiamos patikimumo užtikrinimo paslaugos kvalifikacijos statuso panaikinimą;

(36c) siekiant užtikrinti teisinį tikrumą, kiek tai susiję su kvalifikuotais sertifikatais patvirtintų pažangiųjų elektroninių parašų galiojimu, labai svarbu išsamiai nurodyti, kokias kvalifikuotais sertifikatais patvirtinto pažangiojo elektroninio parašo sudedamąsias dalis turėtų įvertinti tą parašą tvirtinanti pasikliaujančioji šalis;

(36d) patikimumo užtikrinimo paslaugų teikėjai turėtų naudoti kriptografinius algoritmus, atspindinčius dabartinę geriausią praktiką, ir patikimą šių algoritmų įgyvendinimą, kad būtų užtikrintas jų patikimumo užtikrinimo paslaugų saugumas ir patikimumas;

(36e) šiame reglamente turėtų būti nustatyta pareiga kvalifikuotiems patikimumo užtikrinimo paslaugų teikėjams patikrinti fizinio arba juridinio asmens, kuriam išduotas kvalifikuotas sertifikatas, tapatybę remiantis įvairiais suderintais metodais visoje ES. Toks metodas gali apimti kliovimąsi elektroninės atpažinties priemonėmis, kurios atitinka pakankamo saugumo užtikrinimo lygio reikalavimus, kartu pasitelkiant papildomas suderintas nuotolinio ryšio procedūras, kuriomis užtikrinama aukšto patikimumo lygio asmens atpažintis;

(36f) europinių skaitmeninės tapatybės dėklių leidėjai ir elektroninės atpažinties priemonių, apie kurias pranešta, išdavėjai, vykdantys komercinę ar profesinę veiklą, naudodamiesi prieigos valdytojų siūlomomis pagrindinėmis platformos paslaugomis prekių tiekimo ar paslaugų teikimo galutiniams naudotojams tikslu ar jas teikdamas ar tiekdamas, turėtų būti laikomi verslo klientais pagal Reglamento (ES) 2022/1925 2 straipsnio 21 dalį. Todėl prieigos valdytojai turėtų privalėti užtikrinti nemokamą veiksmingą sąveikumą su tos pačios operacinės sistemos, aparatinės ar programinės įrangos funkcijomis, kuriomis jie gali naudotis arba naudojasi teikdami savo pačių papildomas ir palaikymo paslaugas ir aparatinę įrangą, taip pat prieigą prie jų sąveikumo tikslais. Tai turėtų suteikti galimybę europinių skaitmeninės tapatybės dėklių leidėjams ir elektroninės atpažinties priemonių, apie kurias pranešta, išdavėjams per sąsajas ar pasitelkiant panašius sprendimus su atitinkamomis funkcijomis sąveikauti taip pat veiksmingai kaip ir naudojantis paties prieigos valdytojo paslaugomis ar aparatine įranga;

(36g) siekiant, kad šis reglamentas atitiktų dabartinius pokyčius ir būtų laikomasi vidaus rinkos praktikos, Komisijos priimti deleguotieji ir įgyvendinimo aktai turėtų būti peržiūrimi ir prireikus reguliariai atnaujinami. Vertinant šių atnaujinimų būtinumą reikėtų atsižvelgti į vidaus rinkoje atsiradusias naujas technologijas, praktiką, standartus ar technines specifikacijas;

(37) pagal Europos Parlamento ir Tarybos reglamento (ES) 2018/1525[14] 42 straipsnio 1 dalį konsultuotasi su Europos duomenų apsaugos priežiūros pareigūnu;

(38) todėl Reglamentas (ES) Nr. 910/2014 turėtų būti atitinkamai iš dalies pakeistas,

---

14 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39).

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Reglamentas (ES) Nr. 910/2014 iš dalies keičiamas taip:

1) 1 straipsnis pakeičiamas taip:

„Šiuo reglamentu siekiama užtikrinti tinkamą vidaus rinkos veikimą ir tinkamą elektroninės atpažinties priemonių ir patikimumo užtikrinimo paslaugų saugumo lygį. Šiais tikslais šiame reglamente:

aa) nustatomos sąlygos, kuriomis valstybės narės teikia ir pripažįsta fizinių ir juridinių asmenų elektroninės atpažinties priemones, kurioms taikoma kitos valstybės narės elektroninės atpažinties schema, apie kurią pranešta;

ab) nustatomos sąlygos, kuriomis valstybės narės teikia ir pripažįsta europines skaitmeninės tapatybės dėkles;

b) nustatomos patikimumo užtikrinimo paslaugų, visų pirma elektroninių operacijų, taisyklės;

c) nustatoma elektroninių parašų, elektroninių spaudų, elektroninių laiko žymų, elektroninių dokumentų, elektroninio registruoto pristatymo paslaugų, interneto svetainių tapatumo nustatymo sertifikavimo paslaugų, elektroninių parašų, elektroninių spaudų ir jų sertifikatų elektroninio patvirtinimo, interneto svetainių tapatumo nustatymo sertifikatų elektroninio patvirtinimo, elektroninių parašų, elektroninių spaudų ir jų sertifikatų elektroninio išsaugojimo, elektroninio archyvavimo, elektroninio požymių liudijimo, nuotolinio kvalifikuotų elektroninio parašo ir spaudo kūrimo įtaisų administravimo ir elektroninių registrų teisinė sistema;“;

2) 2 straipsnis iš dalies keičiamas taip:

a) 1 dalis pakeičiama taip:

„1. Šis reglamentas taikomas elektroninės atpažinties schemoms, apie kurias pranešė valstybė narė, valstybių narių suteiktoms europinėms skaitmeninės tapatybės dėklėms ir Sąjungoje įsisteigusiems patikimumo užtikrinimo paslaugų teikėjams.“;

b) 3 dalis pakeičiama taip:

„3. Šis reglamentas nedaro poveikio nacionalinės arba Sąjungos teisės aktams, susijusiems su sutarčių sudarymu arba kitų teisinių ar procedūrinių pareigų, susijusių su forma, ar sektoriams taikomais reikalavimų, susijusių su forma, nustatymu ir šių sutarčių ir pareigų bei reikalavimų galiojimu.“;

3) 3 straipsnis iš dalies keičiamas taip:

X) 1 punktas pakeičiamas taip:

„1. elektroninė atpažintis – elektroninių asmens tapatybės duomenų, kuriais nurodomas konkretus fizinis ar juridinis asmuo arba fiziniam ar juridiniam asmeniui atstovaujantis fizinis asmuo, naudojimo procesas;“;

a) 2 punktas pakeičiamas taip:

„2. elektroninės atpažinties priemonė – materialus ir (arba) nematerialus objektas, įskaitant europines skaitmeninės tapatybės dėkles, kuriame yra asmens tapatybės duomenys ir kuris naudojamas asmens, siekiančio naudotis paslauga, tapatumui nustatyti prisijungus arba, kai tinkama, neprisijungus prie interneto;“;

aa) 3 punktas pakeičiamas taip:

„3. asmens tapatybės duomenys – pagal Sąjungos ar nacionalinę teisę suteiktas duomenų rinkinys, pagal kurį galima nustatyti fizinio ar juridinio asmens arba fiziniam ar juridiniam asmeniui atstovaujančio fizinio asmens tapatybę;“;

b) 4 punktas pakeičiamas taip:

„4. elektroninės atpažinties schema – elektroninės atpažinties sistema, pagal kurią fiziniams ar juridiniams asmenims arba fiziniams ar juridiniams asmenims atstovaujantiems fiziniams asmenims išduodamos elektroninės atpažinties priemonės;“;

ba) 5 punktas pakeičiamas taip:

„5. tapatumo nustatymas – elektroninis procesas, leidžiantis patvirtinti fizinio arba juridinio asmens elektroninę atpažintį arba elektroninių duomenų kilmę ir vientisumą;“;

bb) įterpiamas šis 5a punktas:

„5a. naudotojas – fizinis ar juridinis asmuo arba fiziniam ar juridiniam asmeniui atstovaujantis fizinis asmuo, naudojantis pagal šį reglamentą teikiamas patikimumo užtikrinimo paslaugas arba elektroninės atpažinties priemones;“;

c) 14 punktas pakeičiamas taip:

„14. elektroninio parašo sertifikatas – elektroninis liudijimas, kuriuo elektroninio parašo patvirtinimo duomenys susiejami su fiziniu asmeniu ir kuriuo patvirtinamas bent to asmens vardas ir pavardė arba slapyvardis;“;

d) 16 punktas pakeičiamas taip:

„16. patikimumo užtikrinimo paslauga – elektroninė paslauga, kuri paprastai teikiama už atlygį ir kurią sudaro:

a) elektroninių parašų sertifikatų, elektroninių spaudų sertifikatų, interneto svetainių tapatumo nustatymo sertifikatų arba kitų patikimumo užtikrinimo paslaugų teikimo sertifikatų išdavimas;

aa) elektroninių parašų sertifikatų, elektroninių spaudų sertifikatų, interneto svetainių tapatumo nustatymo sertifikatų arba kitų patikimumo užtikrinimo paslaugų teikimo sertifikatų patvirtinimas;

b) elektroninių parašų arba elektroninių spaudų kūrimas;

c) elektroninių parašų arba elektroninių spaudų patvirtinimas;

d) elektroninių parašų, elektroninių spaudų, elektroninių parašų sertifikatų arba elektroninių spaudų sertifikatų išsaugojimas;

e) nuotolinių kvalifikuotų elektroninio parašo kūrimo įtaisų arba nuotolinių kvalifikuotų elektroninio spaudo kūrimo įtaisų administravimas;

f) elektroninių požymių liudijimų išdavimas;

fa) elektroninio požymių liudijimo patvirtinimas;

g) elektroninių laiko žymų sukūrimas;

ga) elektroninių laiko žymų patvirtinimas;

gb) elektroninio registruoto pristatymo paslaugų teikimas;

gc) duomenų, perduodamų naudojantis elektroninio registruoto pristatymo paslaugomis, ir susijusių įrodymų patvirtinimas;

h) elektroninių duomenų elektroninis archyvavimas arba

i) elektroninių duomenų įrašymas į elektroninį registrą;“;

da) 18 punktas pakeičiamas taip:

„18. atitikties vertinimo įstaiga – Reglamento (EB) Nr. 765/2008 2 straipsnio 13 punkte apibrėžta įstaiga, pagal tą reglamentą akredituota kaip kompetentinga įstaiga atlikti kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo ir jo teikiamų kvalifikuotų patikimumo užtikrinimo paslaugų atitikties vertinimą arba atlikti europinių skaitmeninės tapatybės dėklių ar elektroninės atpažinties priemonių sertifikavimą;“;

e) 21 punktas pakeičiamas taip:

„21. produktas – aparatinė arba programinė įranga, arba svarbios aparatinės ir (arba) programinės įrangos sudedamosios dalys, skirtos naudoti teikiant elektroninės atpažinties ir patikimumo užtikrinimo paslaugas;“;

f) įterpiami 23a ir 23b punktai:

„23a. nuotolinis kvalifikuotas elektroninio parašo kūrimo įtaisas – kvalifikuotas elektroninio parašo kūrimo įtaisas, kurį pasirašančiojo vardu pagal 29a straipsnį administruoja kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas;

23b. nuotolinis kvalifikuotas elektroninio spaudo kūrimo įtaisas – kvalifikuotas elektroninio spaudo kūrimo įtaisas, kurį spaudo kūrėjo vardu pagal 39a straipsnį administruoja kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas;“;

g) 29 punktas pakeičiamas taip:

„29. elektroninio spaudo sertifikatas – elektroninis liudijimas, kuriuo elektroninio spaudo patvirtinimo duomenys susiejami su juridiniu asmeniu ir kuriuo patvirtinamas to asmens pavadinimas;“;

h) 41 punktas pakeičiamas taip:

„41. patvirtinimas – patikrinimo ir patvirtinimo, kad elektroniniai duomenys galioja pagal šio reglamento reikalavimus, procedūra;“;

i) įterpiami 42–55b punktai:

„42. europinė skaitmeninės tapatybės dėklė – elektroninės atpažinties priemonė, kuria naudotojui sudaromos sąlygos saugoti ir rasti tapatybės duomenis, be kita ko, asmens tapatybės duomenis, su jų tapatybe susietus elektroninius požymių liudijimus, teikti juos pasikliaujančiosioms šalims šioms prašant ir naudoti juos pagal 6a straipsnį asmens, siekiančio naudotis paslauga, tapatumui nustatyti prisijungus ir, kai tinkama, neprisijungus prie interneto, ir kuria sudaromos sąlygos pasirašyti kvalifikuotu elektroniniu parašu ir užantspauduoti naudojant kvalifikuotus elektroninius spaudus;

43. požymis – fizinio ar juridinio asmens arba objekto ypatybė, savybė, teisė ar leidimas;

44. elektroninis požymių liudijimas – elektroninis liudijimas, pagal kurį galima nustatyti požymių tapatumą;

45. kvalifikuotas elektroninis požymių liudijimas – elektroninis požymių liudijimas, kurį išduoda kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas ir kuris atitinka V priede nustatytus reikalavimus;

45a. elektroninis požymių liudijimas, išduotas už autentišką šaltinį atsakingos viešojo sektoriaus įstaigos arba jos vardu – elektroninis požymių liudijimas, išduotas už autentišką šaltinį atsakingos viešojo sektoriaus įstaigos arba viešojo sektoriaus įstaigos, valstybės narės paskirtos išduoti tokius požymių liudijimus viešojo sektoriaus įstaigų, atsakingų už autentiškus šaltinius pagal 45da straipsnį ir atitinkančių VII priede nustatytus reikalavimus, vardu;

46. autentiškas šaltinis – viešojo sektoriaus įstaigos arba privačiojo subjekto kontroliuojama saugykla arba sistema, kurioje saugomi fizinio ar juridinio asmens požymiai, kuri juos teikia ir kuri laikoma vienu iš pirminių tos informacijos šaltinių arba pagal Sąjungos ar nacionalinę teisę, įskaitant administracinę praktiką, yra pripažįstama autentiška;

47. elektroninis archyvavimas – paslauga, kuria užtikrinamas elektroninių duomenų gavimas, saugojimas, radimas ir šalinimas siekiant garantuoti jų patvarumą ir įskaitomumą, taip pat išsaugoti jų vientisumą, konfidencialumą ir kilmės įrodymą visą saugojimo laikotarpį;

48. kvalifikuota elektroninio archyvavimo paslauga – 45ga straipsnyje nustatytus reikalavimus atitinkanti elektroninio archyvavimo paslauga;

49. ES skaitmeninės tapatybės dėklės patikimumo ženklas – paprastas, atpažįstamas ir aiškus patikrinamas ženklas, kad europinė skaitmeninės tapatybės dėklė suteikta pagal šį reglamentą;

50. saugesnis naudotojo tapatumo nustatymas – suprojektuotas taip, kad būtų apsaugotas tapatumo nustatymo duomenų konfidencialumas, tapatumo nustatymas, kai naudojami bent du tapatumo nustatymo veiksniai iš skirtingų kategorijų: žinojimo (tai, ką žino tik naudotojas), turėjimo (tai, ką turi tik naudotojas) ir būdingumo (tai, kas būdinga naudotojui), kurie yra vienas nuo kito nepriklausomi ir kurių vieną pažeidus kitų patikimumas nesumažėja;

53. elektroninis registras – elektroninių duomenų įrašų seka, kuria užtikrinamas jų vientisumas ir jų chronologinės tvarkos tikslumas;

53a. kvalifikuotas elektroninis registras – 45i straipsnyje nustatytus reikalavimus atitinkantis elektroninis registras;

54. asmens duomenys – bet kokia informacija, kaip apibrėžta Reglamento (ES) 2016/679 4 straipsnio 1 punkte;

55. įrašų atpažintis – procesas, kurio metu asmens tapatybės duomenys, asmens atpažinties priemonės, už autentišką šaltinį atsakingos viešojo sektoriaus įstaigos arba jos vardu išduotas kvalifikuotas elektroninis požymių liudijimas arba požymių liudijimai suderinami arba susiejami su esama tam pačiam asmeniui priklausančia paskyra;

55a. unikalus ir nekintamas identifikatorius – identifikatorius, kurį gali sudaryti vienas arba keli nacionaliniai arba sektoriniai tapatybės duomenys, kuris yra susietas su vienu konkrečios sistemos naudotoju ir yra nekintamas;

55b. duomenų įrašas – elektroniniai duomenys, įrašyti su susijusiais metaduomenimis (arba požymiais), padedančiais tvarkyti duomenis;

55c. europinių skaitmeninės tapatybės dėklių naudojimas neprisijungus prie interneto – naudotojo ir pasikliaujančiosios šalies sąveika fizinėje vietoje, kai sąveikos tikslais nebūtina naudojant dėklę prisijungti prie nuotolinių sistemų elektroninių ryšių tinklais.“

„*5 straipsnis*

Vykdant elektroninę operaciją naudojami slapyvardžiai

Nedarant poveikio slapyvardžiams suteiktai teisinei galiai pagal nacionalinę teisę, vykdant elektronines operacijas nedraudžiama naudoti slapyvardžių.“;

5) II skyriuje prieš 6a straipsnį įterpiama ši antraštė:

„I SKIRSNIS

Europinė skaitmeninės tapatybės dėklė“

7) įterpiami šie 6a, 6b, 6c ir 6d straipsniai:

„*6a straipsnis*

Europinės skaitmeninės tapatybės dėklės

1. Siekiant užtikrinti, kad visi fiziniai ir juridiniai asmenys Sąjungoje turėtų saugią, patikimą ir sklandžią tarpvalstybinę prieigą prie viešųjų ir privačiųjų paslaugų, kiekviena valstybė narė užtikrina, kad per 24 mėnesius nuo 11 dalyje ir 6c straipsnio 4 dalyje nurodytų įgyvendinimo aktų įsigaliojimo dienos būtų suteikta europinė skaitmeninės tapatybės dėklė.

2. Europinės skaitmeninės tapatybės dėklės yra teikiamos:

   a) valstybės narės;

   b) pagal valstybės narės suteiktą įgaliojimą arba

   c) nepriklausomai nuo valstybės narės, bet jai pripažįstant.

3. Europinės skaitmeninės tapatybės dėklės yra elektroninės atpažinties priemonės, kuriomis naudotojui suteikiamos galimybės naudotojui aiškiu ir atsekamu būdu:

   a) saugiai prašyti elektroninių požymių liudijimų bei asmens tapatybės duomenų ir juos pasirinkti, jungti, saugoti, šalinti ir pateikti pasikliaujančiosioms šalims, be kita ko, siekiant prisijungus ir, kai tinkama, neprisijungus prie interneto nustatyti tapatumą, kad būtų galima naudotis viešosiomis ir privačiosiomis paslaugomis, kartu užtikrinant, kad būtų įmanomas pasirinktinis duomenų atskleidimas;

   b) pasirašyti kvalifikuotu elektroniniu parašu ir užantspauduoti naudojant kvalifikuotus elektroninius spaudus.

4. Visų pirma europinėmis skaitmeninės tapatybės dėklėmis:

a) suteikiamas bendras sąsajų rinkinys:

1) siekiant išduoti asmens tapatybės duomenis, kvalifikuotus ir nekvalifikuotus elektroninius požymių liudijimus ar kvalifikuotus ir nekvalifikuotus sertifikatus į europinę skaitmeninės tapatybės dėklę;

2) kad pasikliaujančiosios šalys galėtų prašyti asmens tapatybės duomenų ir elektroninių požymių liudijimų;

3) siekiant prisijungus ir, kai tinkama, neprisijungus prie interneto pateikti asmens tapatybės duomenis ar elektroninį požymių liudijimą pasikliaujančiosioms šalims;

4) kad būtų galima naudotojo sąveika su europine skaitmeninės tapatybės dėkle ir būtų rodomas ES skaitmeninės tapatybės dėklės patikimumo ženklas;

b) elektroninių požymių liudijimų patikimumo užtikrinimo paslaugų teikėjams neteikiama jokia informacija apie šių požymių naudojimą po jų išdavimo;

ba) užtikrinama, kad pasikliaujančiųjų šalių tapatybę būtų galima patvirtinti įgyvendinant tapatumo nustatymo mechanizmus pagal 6b straipsnį;

c) laikomasi 8 straipsnyje nustatytų reikalavimų dėl aukšto saugumo užtikrinimo lygio, mutatis mutandis taikomo asmens tapatybės duomenų administravimui ir naudojimui pasitelkiant dėklę, įskaitant elektroninę atpažintį ir tapatumo nustatymą;

e) užtikrinama, kad 12 straipsnio 4 dalies d punkte nurodyti asmens tapatybės duomenys vienareikšmiškai ir nekintamai nurodytų su dėkle susietą fizinį asmenį, juridinį asmenį arba su dėkle susietam fiziniam ar juridiniam asmeniui atstovaujantį fizinį asmenį.

4a. Valstybės narės numato procedūras, pagal kurias naudotojas galėtų pranešti apie galimą dėklės praradimą ar netinkamą naudojimą ir prašyti ją atšaukti.

5. Valstybės narės įdiegia europinių skaitmeninės tapatybės dėklių patvirtinimo mechanizmus, siekdamos:

a) užtikrinti, kad būtų galima patikrinti dėklės tapatumą ir galiojimą;

d) sudaryti sąlygas naudotojui nustatyti pasikliaujančiųjų šalių tapatumą pagal 6b straipsnį.

6. Europinės skaitmeninės tapatybės dėklės išleidžiamos pagal aukšto saugumo užtikrinimo lygio elektroninės atpažinties schemą, apie kurią pranešta.

6a. Fiziniams asmenims europinės skaitmeninės tapatybės dėklės išduodamos, jie jomis naudojasi tapatumui nustatyti ir jos atšaukiamos nemokamai.

6b. Nedarant poveikio 6db straipsniui, valstybės narės pagal nacionalinę teisę gali numatyti papildomas europinių skaitmeninės tapatybės dėklių funkcijas, įskaitant sąveikumą su esamomis nacionalinėmis elektroninės atpažinties priemonėmis.

7. Naudotojai visiškai kontroliuoja europinės skaitmeninės tapatybės dėklės ir jų europinėje skaitmeninės tapatybės dėklėje esančių duomenų naudojimą. Europinės skaitmeninės tapatybės dėklės leidėjas nerenka informacijos apie dėklės naudotoją, kai ji nėra reikalinga dėklės paslaugoms teikti, ir nejungia asmens tapatybės duomenų bei jokių kitų asmens duomenų, saugomų ar susijusių su europine skaitmeninės tapatybės dėkle, su asmens duomenimis iš bet kokių kitų šio leidėjo siūlomų paslaugų ar iš trečiųjų šalių paslaugų, kurios nėra reikalingos dėklės paslaugoms teikti, naudotojui to aiškiai nepaprašius. Su europinių skaitmeninės tapatybės dėklių suteikimu susiję asmens duomenys saugomi logiškai atskirai nuo bet kokių kitų europinių skaitmeninės tapatybės dėklių leidėjo turimų duomenų. Jei europinę skaitmeninės tapatybės dėklę teikia privačiosios šalys pagal 2 dalies b ir c punktus, mutatis mutandis taikomos 45f straipsnio 4 dalies nuostatos.

7a. Valstybės narės nepagrįstai nedelsdamos pateikia Komisijai informaciją apie:

a) įstaigą, atsakingą už notifikuotųjų pasikliaujančiųjų šalių, kurios kliaujasi europinėmis skaitmeninės tapatybės dėklėmis, sąrašo sudarymą ir tvarkymą pagal 6b straipsnio 2 dalį;

b) įstaigas, atsakingas už europinių skaitmeninės tapatybės dėklių teikimą pagal 6a straipsnio 1 dalį;

c) įstaigas, atsakingas už užtikrinimą, kad asmens tapatybės duomenys būtų susieti su dėkle pagal 6a straipsnio 4 dalies e punktą.

Pranešime taip pat pateikiama informacija apie mechanizmą, pagal kurį galima patvirtinti 12 straipsnio 4 dalyje nurodytus asmens tapatybės duomenis ir pasikliaujančiųjų šalių tapatybę.

Komisija saugiu ryšių kanalu visuomenei pateikia šioje dalyje nurodytą elektroniniu būdu pasirašytą arba užantspauduotą informaciją tokia forma, kad ją būtų galima tvarkyti automatizuotomis priemonėmis.

8. Europinei skaitmeninės tapatybės dėklei mutatis mutandis taikomos 11 straipsnio nuostatos.

9. Europinių skaitmeninės tapatybės dėklių leidėjui mutatis mutandis taikomos 24 straipsnio 2 dalies b, e, g ir h punktų nuostatos.

10. Europinė skaitmeninės tapatybės dėklė turi būti prieinama neįgaliesiems laikantis Direktyvoje 2019/882 nustatytų prieinamumo reikalavimų.

11. Per 6 mėnesius nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktu dėl europinės skaitmeninės tapatybės dėklės įgyvendinimo nustato 3, 4, 5 ir 7a dalyse nurodytų reikalavimų technines ir veikimo specifikacijas bei referencinius standartus. Šis įgyvendinimo aktas priimamas laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

11a. Komisija nustato technines ir veikimo specifikacijas, taip pat referencinius standartus, kad naudotojams būtų lengviau prisijungti prie europinės skaitmeninės tapatybės dėklės naudojant elektroninės atpažinties priemones, atitinkančias aukštą saugumo užtikrinimo lygį, arba elektroninės atpažinties priemones, atitinkančias pakankamą saugumo užtikrinimo lygį, kartu su papildomomis nuotolinio prisijungimo procedūromis, kurios kartu atitinka aukšto saugumo užtikrinimo lygio reikalavimus. Šis įgyvendinimo aktas priimamas laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

6b straipsnis

Europinių skaitmeninės tapatybės dėklių pasikliaujančiosios šalys

1. Privačiąsias ar viešąsias paslaugas teikiančioms pasikliaujančiosioms šalims ketinant kliautis pagal šį reglamentą suteiktomis europinėmis skaitmeninės tapatybės dėklėmis, jos apie tai praneša valstybei narei, kurioje šios pasikliaujančiosios šalys yra įsisteigusios.

1a. Pranešimo procedūra turi būti ekonomiškai efektyvi ir proporcinga rizikai ir ja turi būti užtikrinama, kad pasikliaujančiosios šalys pateiktų bent informaciją, būtiną tapatumui nustatyti jungiantis prie europinių skaitmeninės tapatybės dėklių. Tai turėtų apimti bent valstybę narę, kurioje jos yra įsisteigusios, pasikliaujančiosios šalies vardą ir pavardę / pavadinimą ir, kai taikoma, jos registracijos numerį, kaip nurodyta oficialiuose įrašuose.

1b. Pranešimo reikalavimas nedaro poveikio kitiems pranešimo ir registracijos reikalavimams pagal Sąjungos ar nacionalinę teisę, pavyzdžiui, taikomiems specialių kategorijų asmens duomenų, dėl kurių gali reikėti papildomų leidimo suteikimo reikalavimų, atveju.

1c. Valstybės narės gali atleisti pasikliaujančiąsias šalis nuo reikalavimo pranešti, jei Sąjungos arba nacionalinėje teisėje nėra konkrečių pranešimo ar registracijos reikalavimų, kad jos galėtų susipažinti su informacija, pateikta europinėje skaitmeninės tapatybės dėklėje. Nuo tokio reikalavimo atleistoms pasikliaujančiosioms šalims gali nereikėti įrodyti tapatumo jungiantis prie tos europinės skaitmeninės tapatybės dėklės.

1d. Pasikliaujančiosios šalys, apie kurias pranešta pagal šį straipsnį, nedelsdamos informuoja valstybę narę apie visus vėlesnius iš pradžių pateiktos informacijos pasikeitimus.

2. Pasikliaujančiosios šalys užtikrina 6a straipsnio 4 dalies ba punkte nurodytų tapatumo nustatymo mechanizmų įgyvendinimą.

3. Pasikliaujančiosios šalys atsako už asmenų tapatybės nustatymo ir elektroninio požymių liudijimo, susijusio su europinėmis skaitmeninės tapatybės dėklėmis ir gauto per bendrą sąsają pagal 6a straipsnio 4 dalies a punkto 2 papunktį, patvirtinimo procedūrą.

4. Per 6 mėnesius nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktu dėl europinių skaitmeninės tapatybės dėklių įgyvendinimo, kaip nurodyta 6a straipsnio 11 dalyje, nustato technines ir veikimo 1, 1a ir 1d dalyse nurodytų reikalavimų specifikacijas. Šis įgyvendinimo aktas priimamas laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

6c straipsnis

Europinių skaitmeninės tapatybės dėklių sertifikavimas

1. Europinių skaitmeninės tapatybės dėklių atitiktį 6a straipsnio 3, 4 ir 5 dalyse nustatytiems reikalavimams, 6a straipsnio 7 dalyje nustatytam loginės atskirties reikalavimui ir, kai taikytina, 6a straipsnio 11a dalyje nustatytiems reikalavimams, sertifikuoja pagal Kibernetinio saugumo akto 60 straipsnį akredituotos ir valstybių narių paskirtos atitikties vertinimo įstaigos pagal 4 dalies a, aa ir aaa punktuose nurodytas schemas, specifikacijas, standartus ir procedūras,. Sertifikavimas trunka ne ilgiau kaip penkerius metus, su sąlyga, kad reguliariai atliekamas dvejų metų pažeidžiamumo vertinimas. Nustačius pažeidžiamumą ir per tris mėnesius jo nepašalinus sertifikavimas atšaukiamas.

2. Kalbant apie atitiktį 6a straipsnio 7 dalyje nustatytiems duomenų apsaugos reikalavimams, sertifikavimas pagal 1 dalį gali būti papildytas sertifikavimu pagal Reglamento (ES) 2016/679 42 straipsnį.

3. Europinių skaitmeninės tapatybės dėklių ar jų dalių atitiktį 6a straipsnio 3, 4, 5, 7 ir, kai taikytina, 11a dalyse nustatytiems atitinkamiems kibernetinio saugumo reikalavimams laikydamosi atitinkamų kibernetinio saugumo sertifikavimo schemų pagal Reglamentą (ES) 2019/881, kaip nurodyta 4 dalies a ir aa punktuose, sertifikuoja 1 dalyje nurodytos atitikties vertinimo įstaigos.

3a. Sertifikuotoms europinėms skaitmeninės tapatybės dėklėms netaikomi 7 ir 9 straipsniuose nurodyti reikalavimai.

4. Per 6 mėnesius nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais nustato:

a) kibernetinio saugumo sertifikavimo schemų pagal Reglamentą (ES) 2019/881, reikalingų europinėms skaitmeninės tapatybės dėklėms sertifikuoti, kaip nurodyta 3 dalyje, sąrašą;

aa) specifikacijas, procedūras ir referencinius standartus, skirtus joms naudotis pagal atitinkamas a punkte išvardytas kibernetinio saugumo sertifikavimo schemas;

aaa) specifikacijų, procedūrų ir referencinių standartų, kuriais nustatomi bendri sertifikavimo reikalavimai, kuriems netaikomos atitinkamos kibernetinio saugumo sertifikavimo schemos pagal Reglamentą (ES) 2019/881, sąrašą 1 dalyje nurodyto sertifikavimo tikslais, siekiant įrodyti, kad europinė skaitmeninės tapatybės dėklė atitinka 1 dalyje nurodytus reikalavimus;

b) technines, procedūrines, organizacines ir veikimo specifikacijas, taikomas skiriant 1 dalyje nurodytas atitikties vertinimo įstaigas ir, kiek tai susiję su sertifikavimo reikalavimais, nustatytais pagal aaa punktą, taikomas sertifikavimo schemų ir susijusių vertinimo metodų, kuriuos naudoja šios įstaigos, ir jų išduodamų sertifikatų ir sertifikavimo ataskaitų stebėsenai ir peržiūrai.

5. Valstybės narės praneša Komisijai 1 dalyje nurodytų viešųjų ar privačiųjų įstaigų pavadinimus ir adresus. Komisija tą informaciją pateikia valstybėms narėms.

6. Įgyvendinimo aktai, nurodyti 4 dalyje, priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

6d straipsnis

Sertifikuotų europinių skaitmeninės tapatybės dėklių sąrašo skelbimas

1. Valstybės narės nepagrįstai nedelsdamos informuoja Komisiją apie europines skaitmeninės tapatybės dėkles, kurios yra suteiktos pagal 6a straipsnį ir kurias sertifikavo 6c straipsnio 1 dalyje nurodytos įstaigos. Jos taip pat nepagrįstai nedelsdamos Komisijai praneša apie sertifikavimo atšaukimo atvejus.

2. Remdamasi gauta informacija Komisija sudaro, skelbia ir atnaujina kompiuterio skaitomu formatu pateikiamą sertifikuotų europinių skaitmeninės tapatybės dėklių sąrašą.

3. Per 6 mėnesius nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktu dėl europinių skaitmeninės tapatybės dėklių įgyvendinimo, kaip nurodyta 6a straipsnio 11 dalyje, nustato taikomus formatus ir procedūras 1 ir 2 dalių tikslais. Šis įgyvendinimo aktas priimamas laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

6da straipsnis

Europinių skaitmeninės tapatybės dėklių saugumo pažeidimas

1. Jei pagal 6a straipsnį suteiktos europinės skaitmeninės tapatybės dėklės arba 6a straipsnio 5 dalies a, d ar e punktuose nurodyti patvirtinimo mechanizmai yra pažeisti ar patikimumas pažeistas iš dalies taip, kad yra padarytas poveikis jų patikimumui ar kitų europinių skaitmeninės tapatybės dėklių patikimumui, atitinkamų dėklių leidėjai nepagrįstai nedelsdami sustabdo tos europinės skaitmeninės tapatybės dėklės išdavimą ir naudojimą. Valstybė narė, kurioje buvo suteiktos atitinkamos dėklės, nepagrįstai nedelsdama informuoja valstybes nares ir Komisiją. Atitinkamų dėklių leidėjas arba valstybė narė atitinkamai informuoja pasikliaujančiąsias šalis ir naudotojus.

2. Kai 1 dalyje nurodytas pažeidimas pašalinamas ir patikimumas atkuriamas, dėklės leidėjas atkuria europinės skaitmeninės tapatybės dėklės išleidimą ir naudojimą. Valstybė narė, kurioje buvo suteiktos atitinkamos dėklės, nepagrįstai nedelsdama informuoja valstybes nares ir Komisiją. Atitinkamų dėklių leidėjas arba valstybė narė nepagrįstai nedelsdama informuoja pasikliaujančiąsias šalis ir naudotojus.

3. Jei 1 dalyje nurodytas pažeidimas nepašalinamas ir patikimumas neatkuriamas per tris mėnesius nuo sustabdymo dienos, atitinkama valstybė narė pašalina atitinkamą europinę skaitmeninės tapatybės dėklę iš rinkos ir atitinkamai informuoja kitas valstybes nares ir Komisiją. Kai pateisinama atsižvelgiant į pažeidimo laipsnį, atitinkama europinė skaitmeninės tapatybės dėklė iš rinkos pašalinama nepagrįstai nedelsiant.

4. Atitinkamus 6d straipsnyje nurodyto sąrašo pakeitimus Komisija nepagrįstai nedelsdama skelbia Europos Sąjungos oficialiajame leidinyje.

5. Per 6 mėnesius nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktu dėl europinių skaitmeninės tapatybės dėklių įgyvendinimo, kaip nurodyta 6a straipsnio 11 dalyje, išsamiau nustato 1, 2 ir 3 dalyse nurodytas priemones. Šis įgyvendinimo aktas priimamas laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

6db straipsnis

Tarpvalstybinis kliovimasis europinėmis skaitmeninės tapatybės dėklėmis

1. Kai valstybės narės reikalauja elektroninės atpažinties naudojant elektroninės atpažinties priemonę ir nustatant tapatumą prieigai prie viešojo sektoriaus įstaigos teikiamos internetinės paslaugos, nustatant naudotojo tapatumą jos taip pat pripažįsta pagal šį reglamentą suteiktas europines skaitmeninės tapatybės dėkles.

2. Kai paslaugas teikiančios privačios pasikliaujančiosios šalys, išskyrus labai mažas ir mažąsias įmones, kaip apibrėžta Komisijos rekomendacijoje 2003/361/EB, pagal nacionalinę ar Sąjungos teisę turi užtikrinti saugesnį naudotojo tapatumo nustatymą naudodamos elektroninę atpažintį, ar kai saugesnis naudotojo tapatumo nustatymas būtinas pagal sudarytas sutartis, įskaitant transporto, energetikos, bankininkystės sritis, finansines paslaugas, socialinės apsaugos, sveikatos, geriamojo vandens, pašto paslaugas, skaitmeninės infrastruktūros, švietimo ar telekomunikacijų paslaugas, privačios pasikliaujančiosios šalys ne vėliau kaip per 12 mėnesių nuo europinių skaitmeninės tapatybės dėklių suteikimo pagal 6a straipsnio 1 dalį ir tik naudotojui savanoriškai prašant taip pat sutinka su pagal šį reglamentą suteiktų europinių skaitmeninės tapatybės dėklių naudojimu būtiniausių duomenų, kurių reikia naudojantis konkrečia internetine paslauga, kuri teikiama tik nustačius tapatumą, atžvilgiu.

3. Kai reglamento [SPA reglamento nuoroda] 25 straipsnio 1 dalyje apibrėžtose labai didelėse interneto platformose reikalaujama nustatyti naudotojų tapatumą, kad jie galėtų naudotis internetinėmis paslaugomis, nustatydamos naudotojo tapatumą jos taip pat sutinka su pagal šį reglamentą suteiktų europinių skaitmeninės tapatybės dėklių naudojimu tik naudotojui savanoriškai prašant ir būtiniausių duomenų, kurių reikia naudojantis konkrečia internetine paslauga, kuri teikiama tik nustačius tapatumą, atžvilgiu.

4. Bendradarbiaudama su valstybėmis narėmis Komisija skatina rengti elgesio kodeksus ir sudaro tam sąlygas, siekdama prisidėti prie europinių skaitmeninės tapatybės dėklių plataus prieinamumo ir tinkamumo naudoti šio reglamento taikymo srityje. Šiais elgesio kodeksais palengvinamas elektroninės atpažinties priemonių pripažinimas, įskaitant europines skaitmeninės tapatybės dėkles, kurioms taikomas šis reglamentas, visų pirma, kad jas pripažintų paslaugų teikėjai, pasikliaujantys trečiųjų šalių elektroninės atpažinties paslaugomis naudotojų tapatumui nustatyti. Komisija sudarys sąlygas rengti tokius elgesio kodeksus glaudžiai bendradarbiaudama su visais atitinkamais suinteresuotaisiais subjektais ir skatins paslaugų teikėjus užbaigti rengti elgesio kodeksus per 12 mėnesių nuo šio reglamento priėmimo dienos ir juos veiksmingai įgyvendinti per 18 mėnesių nuo reglamento priėmimo dienos.

5. Per 24 mėnesių nuo europinių skaitmeninės tapatybės dėklių įdiegimo dienos Komisija įvertina, ar remiantis europinės skaitmeninės tapatybės dėklės paklausos, prieinamumo ir tinkamumo naudoti įrodymais papildomi privačiųjų internetinių paslaugų teikėjai turi būti įgalioti pripažinti europinės skaitmeninės tapatybės dėklės naudojimą tik naudotojui savanoriškai to paprašius. Vertinimo kriterijai apima naudotojų bazės mastą, tarpvalstybinį paslaugų teikėjų buvimą, technologijų plėtrą, naudojimo modelių raidą ir vartotojų paklausą.“;

8) prieš 7 straipsnį įterpiama ši antraštė:

„II SKIRSNIS

ELEKTRONINĖS ATPAŽINTIES SCHEMOS“;

9) 7 straipsnio įvadinis sakinys pakeičiamas taip:

„Pagal 9 straipsnio 1 dalį valstybės narės, kurios dar to nepadarė, per 24 mėnesius nuo 6a straipsnio 11 dalyje ir 6c straipsnio 4 dalyje nurodytų įgyvendinimo aktų įsigaliojimo praneša apie bent vieną elektroninės atpažinties schemą, įskaitant bent vieną aukšto saugumo užtikrinimo lygio atpažinties priemonę. Elektroninės atpažinties schema atitinka pranešimo apie ją pagal 9 straipsnio 1 dalį reikalavimus, su sąlyga, kad įvykdomos visos šios sąlygos:“;

10) 9 straipsnio 2 ir 3 dalys pakeičiamos taip:

„2. Komisija Europos Sąjungos oficialiajame leidinyje paskelbia elektroninės atpažinties schemų, apie kurias pranešta pagal šio straipsnio 1 dalį, sąrašą ir pagrindinę informaciją apie šias schemas.

3. 2 dalyje nurodyto sąrašo pakeitimus Komisija per vieną mėnesį nuo to pranešimo gavimo dienos paskelbia Europos Sąjungos oficialiajame leidinyje.“;

12) įterpiamas 11a straipsnis:

„*11a straipsnis*

Įrašų atpažintis

1. Kai tapatumui nustatyti naudojamos elektroninės atpažinties schemos, apie kurias pranešta, arba europinės skaitmeninės tapatybės dėklės, valstybės narės, kai jos veikia kaip pasikliaujančiosios šalys, užtikrina įrašų atpažintį.

2. Europinių skaitmeninės tapatybės dėklių teikimo tikslais valstybės narės į minimalų asmens tapatybės duomenų rinkinį, nurodytą 12 straipsnio 4 dalies d punkte, įtraukia bent vieną unikalų ir nekintamą identifikatorių, kuris atitinka Sąjungos ir nacionalinę teisę, kad būtų galima nustatyti naudotojo tapatybę jam prašant tais atvejais, kai nustatyti jo tapatybę būtina pagal įstatymą.

2a. Valstybės narės numato technines ir organizacines priemones, kad užtikrintų aukštą asmens duomenų, naudojamų atpažįstant įrašus, apsaugos lygį ir užkirstų kelią naudotojų profiliavimui.

2aa. Valstybės narės pagal nacionalinę teisę gali nustatyti, kad europinės skaitmeninės tapatybės dėklės naudotojas gali prašyti, kad unikalus ir nekintamas identifikatorius, įtrauktas į minimalų asmens tapatybės duomenų rinkinį ir susietas su dėkle pagal 6a straipsnio 4 dalies e punktą, būtų pakeistas kitu unikaliu ir nekintamu identifikatoriumi, kurį išdavė valstybė narė.

3. Per 6 mėnesius nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktu išsamiau nustato 1 dalyje nurodytas priemones. Šis įgyvendinimo aktas priimamas laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

3a. Per 6 mėnesius nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktu išsamiau nustato 2 ir 2aa dalyse nurodytas priemones. Šis įgyvendinimo aktas priimamas laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.“;

13) 12 straipsnis iš dalies keičiamas taip:

Bendradarbiavimas ir sąveikumas

a) 3 dalies d punktas išbraukiamas;

b) 4 dalies d punktas pakeičiamas taip:

„d) nuoroda į minimalų asmens tapatybės duomenų rinkinį, būtiną siekiant unikaliai ir nekintamai nurodyti fizinį asmenį, juridinį asmenį arba fizinį asmenį, atstovaujantį fiziniam ir juridiniam asmeniui;“;

ba) 5 dalyje įterpiamas c punktas:

„c) dėl panašaus požiūrio į internetines paslaugas, kurias teikiant pripažįstamos europinės skaitmeninės dėklės, teikiamos pagal šį reglamentą.“;

c) 6 dalies a punktas pakeičiamas taip:

„a) keitimasis elektroninės atpažinties schemų informacija, patirtimi ir gerąja praktika, visų pirma techniniais reikalavimais, susijusiais su sąveikumu, įrašų atpažintimi ir saugumo užtikrinimo lygiais;“;

ca) 6 dalyje įterpiamas e punktas:

„e) keitimasis informacija, patirtimi bei gerąja praktika ir gairių dėl to, kaip internetinės paslaugos gali būti projektuojamos, kuriamos ir įgyvendinamos siekiant pasikliauti europinėmis skaitmeninėmis dėklėmis, teikimas;“;

14) įterpiami šie 12a ir 12b straipsniai:

„*12a straipsnis*

Elektroninės atpažinties schemų sertifikavimas

1. Elektroninės atpažinties schemų, apie kurias reikia pranešti, atitiktis šiame reglamente nustatytiems reikalavimams sertifikuojama siekiant įrodyti tokių schemų ar jų dalių atitiktį 8 straipsnio 2 dalyje nustatytiems reikalavimams dėl elektroninės atpažinties schemų pagal atitinkamą kibernetinio saugumo sertifikavimo schemą pagal Reglamentą (ES) 2019/881 arba pagal tos schemos dalis saugumo užtikrinimo lygių, jei kibernetinio saugumo sertifikatas ar jo dalys apima 8 straipsnio 2 dalyje nustatytus reikalavimus dėl elektroninės atpažinties schemų saugumo užtikrinimo lygių. Sertifikavimas trunka ne ilgiau kaip penkerius metus, su sąlyga, kad reguliariai atliekamas dvejų metų pažeidžiamumo vertinimas. Nustačius pažeidžiamumą ir per tris mėnesius jo nepašalinus sertifikavimas atšaukiamas.

   Sertifikavimą atlieka pagal Reglamentą (EB) Nr. 765/2008 valstybių narių paskirtos akredituotos viešosios arba privačiosios atitikties vertinimo įstaigos.

2. 12 straipsnio 6 dalies c punkte nurodytų elektroninės atpažinties schemų tarpusavio vertinimas netaikomas pagal 1 dalį sertifikuotoms elektroninės atpažinties schemoms ar jų dalims.

2a. Nepaisant šio straipsnio 2 dalies, valstybės narės gali paprašyti pranešančiosios valstybės narės pateikti papildomos informacijos apie elektroninės atpažinties schemas arba jų dalis, sertifikuotas pagal šio straipsnio 2 dalį.

3. Valstybės narės praneša Komisijai 1 dalyje nurodytų viešųjų ar privačiųjų įstaigų pavadinimus ir adresus. Komisija valstybėms narėms užtikrina galimybę gauti tą informaciją.

12b straipsnis

Galimybė naudotis aparatinės ir programinės įrangos funkcijomis

Europinių skaitmeninės tapatybės dėklių leidėjai ir elektroninės atpažinties priemonių, apie kurias pranešta, išdavėjai, vykdantys komercinę ar profesinę veiklą, naudodamiesi pagrindinėmis platformos paslaugomis, nustatytomis Reglamento (ES) 2022/1925 2 straipsnio 2 dalyje, europinės skaitmeninės tapatybės dėklės paslaugų ir elektroninės atpažinties priemonių teikimo galutiniams vartotojams tikslais ar jų teikimo metu yra laikomi verslo klientais pagal Reglamento (ES) 2022/1925 2 straipsnio 21 dalį.“;

17) 13 straipsnio 1 dalis pakeičiama taip:

„1. Nepaisant šio straipsnio 2 dalies, patikimumo užtikrinimo paslaugų teikėjai atsako už tyčia ar dėl neatsargumo fiziniam ar juridiniam asmeniui padarytą žalą dėl pareigų pagal šį reglamentą nevykdymo.

Pareiga įrodyti nekvalifikuoto patikimumo užtikrinimo paslaugų teikėjo tyčią arba neatsargumą tenka fiziniam ar juridiniam asmeniui, reikalaujančiam atlyginti pirmoje pastraipoje nurodytą žalą.

Kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo tyčia ar neatsargumas yra preziumuojami, nebent kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas įrodo, kad pirmoje pastraipoje nurodyta žala padaryta nesant to kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo tyčios ar neatsargumo.“;

18) 14 straipsnis pakeičiamas taip:

„*14 straipsnis*

Tarptautiniai aspektai

1. Trečiojoje valstybėje įsisteigusių patikimumo užtikrinimo paslaugų teikėjų ar tarptautinės organizacijos teikiamos patikimumo užtikrinimo paslaugos pripažįstamos kaip teisiškai lygiavertės Sąjungoje įsisteigusių kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų teikiamoms kvalifikuotoms patikimumo užtikrinimo paslaugoms, kai patikimumo užtikrinimo paslaugos, kurių kilmės šalis yra trečioji valstybė arba tarptautinė organizacija, yra pripažįstamos pagal įgyvendinimo sprendimą arba Sąjungos ir atitinkamos trečiosios valstybės arba tarptautinės organizacijos sudarytą susitarimą pagal Sutarties 218 straipsnį.

2. 1 dalyje nurodytais įgyvendinimo sprendimais ir susitarimais užtikrinama, kad trečiųjų valstybių arba tarptautinių organizacijų patikimumo užtikrinimo paslaugų teikėjai laikytųsi Sąjungoje įsisteigusiems kvalifikuotiems patikimumo užtikrinimo paslaugų teikėjams ir jų teikiamoms kvalifikuotoms patikimumo užtikrinimo paslaugoms taikomų reikalavimų. Trečiosios valstybės ir tarptautinės organizacijos visų pirma sudaro, tvarko ir skelbia pripažintų patikimumo užtikrinimo paslaugų teikėjų patikimą sąrašą.

   1 dalyje nurodytais susitarimais užtikrinama, kad Sąjungoje įsisteigusių kvalifikuotų patikimumo užtikrinimo paslaugos teikėjų teikiamos kvalifikuotos patikimumo užtikrinimo paslaugos būtų pripažįstamos kaip teisiškai lygiavertės trečiųjų valstybių arba tarptautinių organizacijų, su kuriomis sudaryti susitarimai, patikimumo užtikrinimo paslaugų teikėjų teikiamoms patikimumo užtikrinimo paslaugoms.

3. Įgyvendinimo sprendimai, nurodyti 1 dalyje, priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.“;

19) 15 straipsnis pakeičiamas taip:

„*15 straipsnis*

Prieinamumas neįgaliesiems

Patikimumo užtikrinimo paslaugų teikimas ir teikiant šias paslaugas naudojami galutiniams vartotojams skirti gaminiai turi būti prieinami neįgaliesiems laikantis prieinamumo reikalavimų, nurodytų Direktyvoje 2019/882 dėl gaminių ir paslaugų prieinamumo reikalavimų.“;

20) 17 straipsnis iš dalies keičiamas taip:

a) 4 dalis iš dalies keičiama taip:

1) 4 dalies c punktas pakeičiamas taip:

„c) informuoti atitinkamų valstybių narių atitinkamas nacionalines kompetentingas institucijas, paskirtas pagal Direktyvą (ES) XXXX/XXXX [TIS2], apie visus reikšmingus saugumo arba vientisumo pažeidimus, apie kuriuos jos sužino vykdydamos savo užduotis. Jei reikšmingas saugumo arba vientisumo pažeidimas yra susijęs su kitomis valstybėmis narėmis, priežiūros įstaiga informuoja atitinkamos valstybės narės bendrąjį kontaktinį punktą, paskirtą pagal Direktyvą (ES) XXXX/XXXX (TIS2), ir priežiūros įstaigas, paskirtas pagal šio reglamento 17 straipsnį kitose atitinkamose valstybėse narėse. Jei pranešimą gavusi priežiūros įstaiga nustato, kad saugumo ar vientisumo pažeidimo atskleidimas yra svarbus visuomenei, ji informuoja visuomenę arba pareikalauja, kad tą padarytų patikimumo užtikrinimo paslaugų teikėjas;“;

2) f punktas pakeičiamas taip:

„f) bendradarbiauti su kompetentingomis priežiūros institucijomis, įsteigtomis pagal Reglamentą (ES) 2016/679, visų pirma, nepagrįstai nedelsiant jas informuojant, jei atrodo, kad buvo pažeistos asmens duomenų apsaugos taisyklės, ir apie saugumo pažeidimus, kurie atrodo sudarantys asmens duomenų pažeidimus;“;

b) 6 dalis pakeičiama taip:

„6. Kiekviena priežiūros įstaiga kasmet ne vėliau kaip kovo 31 d. pateikia Komisijai ataskaitą apie praėjusiais kalendoriniais metais vykdytą pagrindinę veiklą.“;

c) 8 dalis pakeičiama taip:

„8. Per 12 mėnesių nuo šio reglamento įsigaliojimo Komisija priima gaires dėl priežiūros įstaigų vykdomų 4 dalyje nurodytų užduočių ir įgyvendinimo aktais, priimtais laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros, nustato 6 dalyje nurodytos ataskaitos formatus ir procedūras.“;

21) 18 straipsnis iš dalies keičiamas taip:

a) 18 straipsnio pavadinimas pakeičiamas taip:

„Savitarpio pagalba ir bendradarbiavimas“;

b) 1 dalis pakeičiama taip:

„1. Priežiūros įstaigos bendradarbiauja, siekdamos keistis gerąja praktika ir informacija apie patikimumo užtikrinimo paslaugų teikimą.“;

c) pridedamos 4 ir 5 dalys:

„4. Europos Parlamento ir Tarybos Direktyvoje nustatytos (ES) XXXX/XXXX [TIS2] priežiūros įstaigos ir nacionalinės kompetentingos institucijos bendradarbiauja ir vienos kitoms padeda užtikrinti, kad patikimumo užtikrinimo paslaugų teikėjai laikytųsi šiame reglamente ir Direktyvoje (ES) XXXX/XXXX [TIS2] nustatytų reikalavimų. Priežiūros įstaigos Direktyvoje XXXX/XXXX [TIS2] nustatytų nacionalinių kompetentingų institucijų prašo atlikti priežiūros veiksmus, kad patikrintų, kaip patikimumo užtikrinimo paslaugų teikėjai laikosi Direktyvoje XXXX/XXXX (TIS2) nustatytų reikalavimų, reikalautų, kad patikimumo užtikrinimo paslaugų teikėjai ištaisytų visus šių reikalavimų vykdymo pažeidimus, laiku teiktų visos su patikimumo užtikrinimo paslaugų teikėjais susijusios priežiūros veiklos rezultatus ir informuotų priežiūros institucijas apie atitinkamus incidentus, apie kuriuos pranešta pagal Direktyvą XXXX/XXXX [TIS2].

5. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais nustato būtinus procesinius susitarimus, kuriais palengvinamas 1 dalyje nurodytų priežiūros institucijų bendradarbiavimas. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

21a) įterpiamas 19a straipsnis:

„Nekvalifikuotiems patikimumo užtikrinimo paslaugų teikėjams keliami reikalavimai

1. Nekvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, teikiantis nekvalifikuotas patikimumo užtikrinimo paslaugas:

a) taiko tinkamą politiką ir imasi atitinkamų su nekvalifikuotos patikimumo užtikrinimo paslaugos teikimu susijusios teisinės, verslo, veiklos ir kitos tiesioginės ar netiesioginės rizikos valdymo priemonių. Nepaisant Direktyvos (ES) XXXX/XXX [TIS2] 18 straipsnio nuostatų, šios priemonės apima bent šias priemones:

i) su paslaugos registravimu ir prisijungimo prie paslaugos procedūromis susijusias priemones;

ii) su procesiniais ar administraciniais patikrinimais susijusias priemones;

iii) su paslaugų administravimu ir įgyvendinimu susijusias priemones;

b) praneša priežiūros įstaigai, poveikį patyrusiems asmenims, kurių tapatybė gali būti nustatyta, ir visuomenei, jei tai susiję su viešuoju interesu, ir, kai taikytina, kitoms atitinkamoms kompetentingoms įstaigoms apie visus paslaugų teikimo pažeidimus ar sutrikimus arba a punkto i, ii ir iii papunkčiuose nurodytų priemonių įgyvendinimo pažeidimus ar sutrikimus, kurie daro didelį poveikį teikiamai patikimumo užtikrinimo paslaugai arba joje saugomiems asmens duomenims nepagrįstai nedelsdama ir bet kuriuo atveju ne vėliau kaip per 24 valandas nuo tada, kai apie tai sužino.

2. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais konkrečiai nustato 1 dalies a punkte nurodytų priemonių techninius požymius. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

22) 20 straipsnis iš dalies keičiamas taip:

a) 1 dalis pakeičiama taip:

„1. Atitikties vertinimo įstaiga atlieka kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų auditą jų lėšomis bent kas 24 mėnesius. Auditas patvirtina, kad kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai ir jų teikiamos kvalifikuotos patikimumo užtikrinimo paslaugos atitinka šiame reglamente ir Direktyvos (ES) XXXX/XXXX [TIS2] 18 straipsnyje nustatytus reikalavimus. Kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai po to parengtą atitikties įvertinimo ataskaitą priežiūros įstaigai pateikia per tris darbo dienas nuo jos gavimo dienos.“;

aa) įterpiama ši dalis:

„1a. Valstybės narės gali nustatyti, kad kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai turi iš anksto informuoti priežiūros įstaigą apie planuojamus auditus ir leistų priežiūros įstaigai, jai paprašius, dalyvauti stebėtojo teisėmis.“;

b) 2 dalies paskutinis sakinys pakeičiamas taip:

„Kai nustatoma, kad buvo pažeistos asmens duomenų apsaugos taisyklės, priežiūros įstaiga nepagrįstai nedelsdama apie tai praneša Reglamente (ES) 2016/679 nurodytoms priežiūros institucijoms.“;

c) 3 ir 4 dalys pakeičiamos taip:

„3. Kvalifikuotam patikimumo užtikrinimo paslaugų teikėjui neįvykdžius šiame reglamente nustatytų reikalavimų, priežiūros įstaiga reikalauja, kad jis ištaisytų reikalavimų vykdymo pažeidimą per nustatytą laikotarpį, jei taikytina.

Jei tas teikėjas pažeidimo nepašalina, jei taikytina, per priežiūros įstaigos nustatytą laikotarpį, priežiūros įstaiga, atsižvelgdama visų pirma į tokio pažeidimo mastą, trukmę ir pasekmes, gali panaikinti to teikėjo arba paveiktos jo teikiamos paslaugos kvalifikacijos statusą.

3a. Jeigu nacionalinės kompetentingos institucijos priežiūros įstaigą informuoja pagal Direktyvą (ES) XXXX/XXXX [TIS2], kad kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas nevykdo kurio nors iš Direktyvos (ES) XXXX/XXXX [TIS2] 18 straipsnyje nustatytų reikalavimų, priežiūros įstaiga, visų pirma atsižvelgdama į to nesilaikymo mastą, trukmę ir pasekmes, gali panaikinti to teikėjo arba atitinkamos paveiktos jo teikiamos paslaugos kvalifikacijos statusą.

3b. Jeigu priežiūros institucijos priežiūros įstaigą informuoja pagal Reglamentą (ES) 2016/679, kad kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas nevykdo kurio nors iš Reglamente (ES) 2016/679 nustatytų reikalavimų, priežiūros įstaiga, visų pirma atsižvelgdama į to nesilaikymo mastą, trukmę ir pasekmes, gali panaikinti to teikėjo arba paveiktos jo teikiamos paslaugos kvalifikacijos statusą.

3c. Priežiūros įstaiga informuoja kvalifikuotą patikimumo užtikrinimo paslaugų teikėją apie jo kvalifikacijos statuso arba atitinkamos paslaugos kvalifikacijos statuso panaikinimą. Priežiūros įstaiga informuoja 22 straipsnio 3 dalyje nurodytą įstaigą 22 straipsnio 1 dalyje patikimų sąrašų naujinimo tikslais ir nacionalinę kompetentingą instituciją, nurodytą Direktyvoje XXXX [TIS2].

4. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais nustato technines specifikacijas ir standartų referencinius numerius dėl:

a) atitikties vertinimo įstaigų akreditavimo ir 1 dalyje nurodytos atitikties vertinimo ataskaitos;

b) audito reikalavimų atitikties vertinimo įstaigoms atlikti kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų atitikties vertinimą kaip nurodyta 1 dalyje;

c) atitikties vertinimo schemų, pagal kurias atitikties vertinimo įstaigos atlieka kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų atitikties vertinimą ir teikia 1 dalyje nurodytą ataskaitą.

Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

23) 21 straipsnis iš dalies keičiamas taip:

„1. Jeigu patikimumo užtikrinimo paslaugų teikėjai ketina pradėti teikti kvalifikuotą patikimumo užtikrinimo paslaugą, jie priežiūros įstaigai pateikia pranešimą apie savo ketinimą kartu su atitikties vertinimo įstaigos parengta atitikties vertinimo ataskaita, kuria patvirtinama, kad laikomasi šiame reglamente ir Direktyvos (ES) XXXX/XXXX [TIS2] 18 straipsnyje nustatytų reikalavimų.“;

a) 2 dalis pakeičiama taip:

„2. Priežiūros įstaiga patikrina, ar patikimumo užtikrinimo paslaugų teikėjas ir jo teikiamos patikimumo užtikrinimo paslaugos atitinka šiame reglamente nustatytus reikalavimus, ypač kvalifikuotiems patikimumo užtikrinimo paslaugų teikėjams ir jų teikiamoms kvalifikuotoms patikimumo užtikrinimo paslaugoms taikomus reikalavimus.

Siekdama patikrinti patikimumo užtikrinimo paslaugų teikėjo atitiktį Direktyvos XXXX [TIS2] 18 straipsnyje nustatytiems reikalavimams, priežiūros įstaiga prašo Direktyvoje XXXX [TIS2] nurodytų kompetentingų institucijų tuo tikslu atlikti priežiūros veiksmus ir pateikti informaciją apie rezultatus nepagrįstai nedelsiant ir ne vėliau kaip per du mėnesius nuo dienos, kai Direktyvoje XXXX [TIS2] nurodytos kompetentingos institucijos gauna šį prašymą. Jeigu per du mėnesius nuo pranešimo dienos patikrinimas nebaigiamas, Direktyvoje XXXX [TIS2] nurodytos kompetentingos institucijos informuoja priežiūros įstaigą nurodydamos vėlavimo priežastis ir laikotarpį, per kurį patikrinimas bus baigtas.

Jei priežiūros įstaiga padaro išvadą, kad patikimumo užtikrinimo paslaugų teikėjas ir jo teikiamos patikimumo užtikrinimo paslaugos atitinka šiame reglamente nustatytus reikalavimus, ji suteikia jam kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo, o jo teikiamoms paslaugoms – kvalifikuotų patikimumo užtikrinimo paslaugų statusą ir ne vėliau kaip per tris mėnesius nuo pranešimo pateikimo pagal šio straipsnio 1 dalį dienos apie tai praneša 22 straipsnio 3 dalyje nurodytai įstaigai, kad būtų galima atnaujinti 22 straipsnio 1 dalyje nurodytus patikimus sąrašus.

Jeigu per tris mėnesius nuo pranešimo dienos patikrinimas nebaigiamas, priežiūros įstaiga apie tai praneša patikimumo užtikrinimo paslaugų teikėjui, nurodydama vėlavimo priežastis ir laikotarpį, per kurį patikrinimas bus baigtas.“;

b) 4 dalis pakeičiama taip:

„4. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais nustato pranešimo ir tikrinimo pagal 1 ir 2 dalis formatus ir procedūras. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

25) 24 straipsnis iš dalies keičiamas taip:

a) 1 dalis pakeičiama taip:

„1. Išduodamas kvalifikuotą sertifikatą arba kvalifikuotą patikimumo užtikrinimo paslaugos elektroninį požymių liudijimą, kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas patikrina fizinio ar juridinio asmens, kuriam bus išduotas kvalifikuotas sertifikatas arba kvalifikuotas elektroninis požymių liudijimas, tapatybę ir, jeigu taikytina, visus jo specifinius požymius.

Pirmoje pastraipoje nurodytą informaciją kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas tikrina tiesiogiai arba paveda tai atlikti trečiajai šaliai bet kuriuo toliau nurodytu būdu:

a) naudodamas europinę skaitmeninės tapatybės dėklę arba elektroninės atpažinties priemones, apie kurias pranešta ir kurios atitinka 8 straipsnyje nustatytus reikalavimus aukšto saugumo užtikrinimo lygio;

b) naudodamas pagal a, c arba d punktą išduotą kvalifikuotą elektroninį požymių liudijimą, kvalifikuoto elektroninio parašo arba kvalifikuoto elektroninio spaudo sertifikatą;

c) naudodamas kitus tapatybės nustatymo būdus, kuriais užtikrinamas aukšto patikimumo lygio asmens tapatybės nustatymas, kurio atitiktį turi patvirtinti atitikties vertinimo įstaiga;

d) fiziškai dalyvaujant fiziniam asmeniui arba juridinio asmens įgaliotajam atstovui vykdant tinkamas procedūras ir laikantis nacionalinių teisės aktų.“;

b) įterpiama 1a dalis:

„1a. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais nustato minimalias technines specifikacijas, standartus ir procedūras dėl tapatybės ir požymių patikrinimo pagal 1 dalies c punktą. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

c) 2 dalis iš dalies keičiama taip:

0) a punktas iš dalies keičiamas taip:

„a) informuoja priežiūros įstaigą bent prieš mėnesį iki bet kokio jos kvalifikuotų patikimumo užtikrinimo paslaugų teikimo pakeitimo arba bent prieš tris mėnesius, jei ketinama nutraukti tą veiklą. Prieš suteikdama leidimą įgyvendinti numatytus kvalifikuotų patikimumo užtikrinimo paslaugų pakeitimus, priežiūros įstaiga gali paprašyti pateikti papildomos informacijos arba atitikties vertinimo rezultatus. Jeigu per tris mėnesius nuo pranešimo dienos patikrinimas nebaigiamas, priežiūros įstaiga apie tai praneša patikimumo užtikrinimo paslaugų teikėjui, nurodydama vėlavimo priežastis ir laikotarpį, per kurį patikrinimas bus baigtas.“;

1) d ir e punktai pakeičiami taip:

„d) prieš užmegzdamas sutartinius santykius, aiškiai, išsamiai ir lengvai prieinamu būdu viešai prieinamoje erdvėje ir atskirai informuoja visus asmenis, kurie nori naudotis kvalifikuota patikimumo užtikrinimo paslauga, apie tikslias naudojimosi ta paslauga sąlygas, įskaitant visus naudojimosi ja apribojimus;

e) naudoja patikimas sistemas ir produktus, kurie yra apsaugoti nuo pakeitimų, ir užtikrina jų palaikomų procesų techninį saugumą ir patikimumą, be kita ko, naudodamas tinkamus kriptografinius algoritmus, raktų ilgius ir maišos funkcijas sistemose, produktuose ir jų palaikomuose procesuose;“;

2) įterpiami nauji fa ir fb punktai:

„fa) taiko tinkamą politiką ir imasi atitinkamų su kvalifikuotos patikimumo užtikrinimo paslaugos teikimu susijusios teisinės, verslo, veiklos ir kitos tiesioginės ar netiesioginės rizikos valdymo priemonių. Nepaisant Direktyvos (ES) XXXX/XXX [TIS2] 18 straipsnio nuostatų, šios priemonės apima bent šias priemones:

i) su paslaugos registravimu ir prisijungimo prie paslaugos procedūromis susijusias priemones;

ii) su procesiniais ar administraciniais patikrinimais susijusias priemones;

iii) su paslaugų administravimu ir įgyvendinimu susijusias priemones;

fb) praneša priežiūros įstaigai, poveikį patyrusiems asmenims, kurių tapatybė gali būti nustatyta, kitoms susijusioms kompetentingoms įstaigoms, kai taikytina, ir, priežiūros įstaigos prašymu, visuomenei, jei tai susiję su viešuoju interesu, apie visus paslaugų teikimo pažeidimus ar sutrikimus arba fa punkto i, ii ir iii papunkčiuose nurodytų priemonių įgyvendinimo pažeidimus ar sutrikimus, kurie daro didelį poveikį teikiamai patikimumo užtikrinimo paslaugai arba joje saugomiems asmens duomenims nepagrįstai nedelsdama ir bet kuriuo atveju ne vėliau kaip per 24 valandas po incidento;“;

3) g ir h punktai pakeičiami taip:

„g) imasi tinkamų priemonių, kad apsisaugotų nuo duomenų klastojimo, vagystės ar pasisavinimo, neteisėto duomenų šalinimo, keitimo ar prieigos prie kompiuterinių duomenų užkirtimo;

h) tiek, kiek reikia, kvalifikuotam patikimumo užtikrinimo paslaugų teikėjui nutraukus veiklą, registruoja ir laiko prieinamą visą susijusią informaciją dėl kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo parengtų ir gautų duomenų tam, kad šią informaciją būtų galima panaudoti teismo procese kaip įrodymą ir siekiant užtikrinti paslaugų tęstinumą. Toks registravimas gali būti atliekamas elektroniniu būdu;“;

4) j punktas išbraukiamas;

d) įterpiama 4a dalis:

„4a. Kvalifikuotų elektroninių požymių liudijimų atšaukimui atitinkamai taikomos 3 ir 4 dalys.“;

e) 5 dalis pakeičiama taip:

„5. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais nustato 2 dalyje nurodytų reikalavimų technines specifikacijas, procedūras ir standartų referencinius numerius. Jeigu atitinkamos techninės specifikacijos, procedūros ir standartai, laikoma, kad užtikrinta atitiktis šio straipsnio reikalavimams. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

f) įterpiama 6 dalis:

„6. Komisijai suteikiami įgaliojimai priimti įgyvendinimo aktus, konkrečiai nustatant 2 dalies fa punkte nurodytų priemonių techninius požymius.“;

25a) 26 straipsnis iš dalies keičiamas taip:

„2. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais nustato pažangiųjų elektroninių parašų technines specifikacijas ir standartų referencinius numerius. Jeigu pažangusis elektroninis parašas atitinka tas specifikacijas ir standartus, laikoma, kad užtikrinta atitiktis pažangiesiems elektroniniams parašams nustatytiems reikalavimams. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

25b) 27 straipsnis iš dalies keičiamas taip:

4 dalis išbraukiama.

26) 28 straipsnio 6 dalis pakeičiama taip:

„6. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais nustato elektroninių parašų kvalifikuotų sertifikatų technines specifikacijas ir standartų referencinius numerius. Jeigu kvalifikuotas elektroninio parašo sertifikatas atitinka tas specifikacijas ir standartus, laikoma, kad užtikrinta atitiktis I priede nustatytiems reikalavimams. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

27) 29 straipsnis papildomas nauja 1a dalimi:

„1a. Kurti, administruoti elektroninio parašo kūrimo duomenis pasirašančiojo vardu arba kopijuoti tokio parašo sukūrimo duomenis atsarginės kopijos tikslais gali tik kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, teikiantis kvalifikuotą patikimumo užtikrinimo paslaugą, susijusią su nuotolinio kvalifikuoto elektroninio parašo kūrimo įtaiso administravimu.“;

28) Įterpiamas 29a straipsnis:

„*29a straipsnis*

Kvalifikuotai nuotolinių kvalifikuoto elektroninio parašo kūrimo įtaisų administravimo paslaugai taikomi reikalavimai

1. Nuotolinius kvalifikuoto elektroninio parašo kūrimo įtaisus administruoti kaip kvalifikuotą paslaugą gali tik kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, kuris:

   a) pasirašančiojo vardu kuria ar administruoja elektroninio parašo kūrimo duomenis;

   b) nepaisydamas II priedo 1 dalies d punkto nuostatų gali kopijuoti elektroninio parašo kūrimo duomenis tik atsarginės kopijos tikslais, jei laikomasi šių reikalavimų:

      i. duomenų rinkinių kopijų saugumo lygis turi būti toks pat kaip originalių duomenų rinkinių;

      ii. duomenų rinkinių kopijų negali būti daugiau nei būtina norint užtikrinti paslaugos tęstinumą;

   c) laikosi visų reikalavimų, nustatytų pagal 30 straipsnį išduoto konkretaus nuotolinio kvalifikuoto parašo kūrimo įtaiso sertifikavimo ataskaitoje.

2. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais nustato taikant 1 dalį naudotinas technines specifikacijas ir standartų referencinius numerius.“;

29) 30 straipsnyje įterpiama 3a dalis:

„3a. 1 dalyje nurodyto sertifikavimo galiojimas neviršija 5 metų priklausomai nuo reguliaraus kas 2 metus atliekamo pažeidžiamumo vertinimo. Nustačius pažeidžiamumą ir jo nepašalinus sertifikavimas panaikinamas.“;

30) 31 straipsnio 3 dalis pakeičiama taip:

„3. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais nustato taikant 1 dalį naudotinus formatus ir procedūras. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

31) 32 straipsnis iš dalies keičiamas taip:

a) 1 dalis papildoma šia pastraipa:

„Jeigu kvalifikuotų elektroninių parašų galiojimo patvirtinimas atitinka 3 dalyje nurodytas specifikacijas ir standartus, laikoma, kad užtikrinta atitiktis pirmoje pastraipoje nustatytiems reikalavimams.“;

b) 3 dalis pakeičiama taip:

„3. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais pateikia kvalifikuotų elektroninių parašų patvirtinimo specifikacijas ir standartų referencinius numerius. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

31a) įterpiamas 32a straipsnis:

„Pažangių elektroninių parašų, pagrįstų kvalifikuotais sertifikatais, patvirtinimo reikalavimai

1. Pažangiojo elektroninio parašo, pagrįsto kvalifikuotu sertifikatu, galiojimo patvirtinimo procedūra patvirtinamas pažangiojo elektroninio parašo, pagrįsto kvalifikuotu sertifikatu, galiojimas su sąlyga, kad:

a) sertifikatas, kuriuo tvirtinamas parašas, pasirašymo metu buvo kvalifikuotas elektroninio parašo sertifikatas, atitinkantis I priedą;

b) kvalifikuotą sertifikatą išdavė kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas ir jis galiojo pasirašymo metu;

c) parašo patvirtinimo duomenys atitinka pasikliaujančiajai šaliai pateiktus duomenis;

d) unikalus duomenų, kuriais sertifikate nurodomas pasirašantis asmuo, rinkinys tinkamai pateikiamas pasikliaujančiajai šaliai;

e) jei pasirašymo metu buvo naudojamas slapyvardis, tai aiškiai nurodoma pasikliaujančiajai šaliai;

f) nebuvo pažeistas pasirašytų duomenų vientisumas;

g) pasirašymo metu buvo laikomasi 26 straipsnyje nurodytų reikalavimų. Jeigu pažangiųjų elektroninių parašų, pagrįstų kvalifikuotais sertifikatais, galiojimo patvirtinimas atitinka 3 dalyje nurodytas specifikacijas ir standartus, laikoma, kad užtikrinta atitiktis pirmoje pastraipoje nustatytiems reikalavimams.

2. Sistema, naudojama pažangiojo elektroninio parašo, pagrįsto kvalifikuotu sertifikatu, galiojimo patvirtinimo tikslais, duoda pasikliaujančiajai šaliai teisingą galiojimo patvirtinimo procedūros rezultatą ir leidžia pasikliaujančiai šaliai nustatyti bet kokias su saugumu susijusias problemas.

3. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais pateikia pažangiųjų elektroninių parašų, pagrįstų kvalifikuotais sertifikatais, galiojimo patvirtinimo specifikacijas ir standartų referencinius numerius. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“

31b) 33 straipsnis iš dalies keičiamas taip:

„1. Kvalifikuotų elektroninių parašų kvalifikuotą galiojimo patvirtinimo paslaugą gali teikti tik kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, kuris:“;

„2. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais nustato 1 dalyje nurodytų kvalifikuotų galiojimo patvirtinimo paslaugų technines specifikacijas ir standartų referencinius numerius. Jeigu kvalifikuoto elektroninio parašo galiojimo patvirtinimo paslauga atitinka tas specifikacijas ir standartus, laikoma, kad užtikrinta atitiktis 1 dalyje nustatytiems reikalavimams. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“

32) 34 straipsnis pakeičiamas taip:

„*34 straipsnis*

Kvalifikuota kvalifikuotų elektroninių parašų ilgalaikio išsaugojimo paslauga

1. Kvalifikuotą kvalifikuotų elektroninių parašų ilgalaikio išsaugojimo paslaugą gali teikti tik kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, taikantis procedūras ir metodus, kuriais galima toliau užtikrinti kvalifikuoto elektroninio parašo patikimumą pasibaigus technologinio galiojimo laikotarpiui.

2. Jeigu kvalifikuotos kvalifikuotų elektroninių parašų ilgalaikio išsaugojimo paslaugos priemonės atitinka 3 dalyje nurodytas specifikacijas ir standartus, laikoma, kad užtikrinta atitiktis 1 dalyje nustatytiems reikalavimams.

3. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais nustato kvalifikuotos kvalifikuotų elektroninių parašų ilgalaikio išsaugojimo paslaugos technines specifikacijas ir standartų referencinius numerius. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

32a) 36 straipsnis papildomas nauja 2 dalimi:

„2. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais nustato pažangiųjų elektroninių spaudų technines specifikacijas ir standartų referencinius numerius.

Jeigu pažangusis elektroninis spaudas atitinka tas specifikacijas ir standartus, laikoma, kad užtikrinta atitiktis pažangiesiems elektroniniams spaudams nustatytiems reikalavimams. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

33) 37 straipsnis iš dalies keičiamas taip:

4 dalis išbraukiama.

34) 38 straipsnis iš dalies keičiamas taip:

a) 1 dalis pakeičiama taip:

„1. Kvalifikuoti elektroninių spaudų sertifikatai turi atitikti III priede nustatytus reikalavimus. Jeigu kvalifikuotas elektroninio spaudo sertifikatas atitinka 6 dalyje nurodytas specifikacijas ir standartus, laikoma, kad užtikrinta atitiktis III priede nustatytiems reikalavimams.“;

b) 6 dalis pakeičiama taip:

„6. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais nustato kvalifikuotų elektroninių spaudų sertifikatų technines specifikacijas ir standartų referencinius numerius. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

35) įterpiamas 39a straipsnis:

„*39a straipsnis*

Kvalifikuotai nuotolinių kvalifikuoto elektroninio spaudo kūrimo įtaisų administravimo paslaugai taikomi reikalavimai

Kvalifikuotai nuotolinių kvalifikuoto elektroninio spaudo kūrimo įtaisų administravimo paslaugai mutatis mutandis taikomas 29a straipsnis.“;

35a) įterpiamas 40a straipsnis:

„*40a straipsnis*

Kvalifikuotais sertifikatais pagrįstų pažangiųjų elektroninių spaudų patvirtinimo reikalavimai

(1) Kvalifikuotais sertifikatais pagrįstų pažangiųjų elektroninių spaudų patvirtinimui *mutatis mutandis* taikomas 32a straipsnis.“;

36) 42 straipsnis iš dalies keičiamas taip:

a) pridedama nauja 1a dalis:

„1a. Jeigu datos ir laiko susiejimas su duomenimis ir tikslus laiko šaltinis atitinka 2 dalyje nurodytas specifikacijas ir standartus, laikoma, kad užtikrinta atitiktis 1 dalyje nustatytiems reikalavimams.“;

b) 2 dalis pakeičiama taip:

„2. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais nustato datos ir laiko susiejimo su duomenimis ir tikslių laiko šaltinių technines specifikacijas ir standartų referencinius numerius. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

36a) 43 straipsnis papildomas nauja 3 dalimi:

„2a. Kvalifikuota elektroninio registruoto pristatymo paslauga, teikiama vienoje valstybėje narėje, pripažįstama kvalifikuota elektroninio registruoto pristatymo paslauga bet kurioje kitoje valstybėje narėje.“;

37) 44 straipsnis iš dalies keičiamas taip:

a) įterpiama 1a dalis:

„1a. Jeigu duomenų siuntimo ir gavimo procesas atitinka 2 dalyje nurodytas specifikacijas ir standartus, laikoma, kad užtikrinta atitiktis 1 dalyje nustatytiems reikalavimams.“;

b) 2 dalis pakeičiama taip:

„2. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais nustato duomenų siuntimo ir gavimo proceso technines specifikacijas ir standartų referencinius numerius. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

c) įterpiamos 3 ir 4 dalys:

„3. Kvalifikuotų elektroninio registruoto pristatymo paslaugų teikėjai gali susitarti dėl savo teikiamų kvalifikuotų elektroninio registruoto pristatymo paslaugų sąveikumo. Tokia sąveikumo sistema turi atitikti 1 dalyje išdėstytus reikalavimus. Atitiktį turi patvirtinti atitikties vertinimo įstaiga.“;

„4. Siekdama palengvinti duomenų perdavimą tarp dviejų ar daugiau kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų, Komisija įgyvendinimo aktu gali nustatyti technines specifikacijas ir standartų referencinius numerius. Techninės specifikacijos ir standartų turinys turi būti ekonomiškai efektyvūs ir proporcingi. Įgyvendinimo aktas priimamas pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

38) 45 straipsnis pakeičiamas taip:

„*45 straipsnis*

Kvalifikuotų interneto svetainės tapatumo nustatymo sertifikatų reikalavimai

1. Kvalifikuoti interneto svetainių tapatumo nustatymo sertifikatai turi atitikti IV priede nustatytus reikalavimus. Atitiktis IV priede nustatytiems reikalavimams vertinama pagal 4 dalyje nurodytas specifikacijas ir standartus.

2. 1 dalyje nurodyti kvalifikuoti interneto svetainių tapatumo nustatymo sertifikatai turi būti pripažįstami interneto naršyklėse. Šiais tikslais interneto naršyklėse būtina užtikrinti, kad bet kuriuo metodu pateikti tapatybės duomenys būtų rodomi naudotojui patogiu būdu. Interneto naršyklėse turi būti užtikrintas suderinamumas ir sąveikumas su 1 dalyje nurodytais kvalifikuotais interneto svetainės tapatumo nustatymo sertifikatais, išskyrus įmones, kurios laikomos labai mažomis įmonėmis, ir mažas įmones pagal Komisijos rekomendaciją 2003/361/EB per pirmuosius 5 interneto naršymo paslaugų teikėjų veiklos metus.

4. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais pateikia 1 ir 2 dalyse nurodytų kvalifikuotų interneto svetainės tapatumo nustatymo sertifikatų specifikacijas ir standartų referencinius numerius. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

39) po 45 straipsnio įterpiami 9, 10 ir 11 skirsniai:

„9 SKIRSNIS

ELEKTRONINIS POŽYMIŲ LIUDIJIMAS

45a straipsnis

Elektroninio požymių liudijimo teisinė galia

1. Negalima atsisakyti pripažinti elektroninio požymių liudijimo teisinės galios ir jo tinkamumo naudoti kaip įrodymo teismo procese tik dėl to, kad jis yra elektroninis arba kad jis neatitinka kvalifikuotų elektroninių požymių liudijimų reikalavimų.

2. Už autentišką šaltinį atsakingos viešojo sektoriaus įstaigos arba jos vardu išduotas kvalifikuotas elektroninis požymių liudijimas ir požymių liudijimai turi tokią pačią teisinę galią kaip teisėtai išduoti popieriniai liudijimai.

3. Kvalifikuotas elektroninis požymių liudijimas, išduotas vienoje valstybėje narėje, pripažįstamas kvalifikuotu elektroniniu požymių liudijimu bet kurioje kitoje valstybėje narėje.

4. Už autentišką šaltinį atsakingos viešojo sektoriaus įstaigos arba jos vardu išduotas požymių liudijimas pripažįstamas už autentišką šaltinį atsakingos viešojo sektoriaus įstaigos arba jos vardu išduotu požymių liudijimu visose valstybėse narėse.

45b straipsnis

Elektroninis požymių liudijimas teikiant viešąsias paslaugas

Kai pagal nacionalinės teisės aktus reikalaujama, kad norint valstybėje narėje pasinaudoti viešojo sektoriaus įstaigos teikiama internetine paslauga būtina užtikrinti elektroninę atpažintį naudojant elektroninės atpažinties priemones ir tapatumo nustatymą, elektroniniame požymių liudijime esantys asmens tapatybės duomenys neatstoja elektroninės atpažinties naudojant elektroninės atpažinties priemones ir tapatumo nustatymą, jei tai nėra konkrečiai leidusi valstybė narė. Tokiu atveju pripažįstami ir kitų valstybių narių kvalifikuoti elektroniniai požymių liudijimai. straipsnis

45c straipsnis

Kvalifikuotų elektroninių požymių liudijimų reikalavimai

1. Kvalifikuoti elektroninių požymių liudijimai turi atitikti V priede nustatytus reikalavimus.

1a. Atitiktis V priede nustatytiems reikalavimams vertinama pagal 4 dalyje nurodytas specifikacijas ir standartus.

2. Be V priede nustatytų reikalavimų, kvalifikuotiems elektroniniams požymių liudijimams netaikoma jokių privalomų reikalavimų.

3. Jeigu iš pradžių išduotas kvalifikuotas elektroninis požymių liudijimas vėliau atšaukiamas, jis netenka galios nuo jo atšaukimo momento, o jo statuso jokiomis aplinkybėmis negalima atkurti.

4. Per 6 mėnesius nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktu dėl europinių skaitmeninės tapatybės dėklių įgyvendinimo, kaip nurodyta 6a straipsnio 11 dalyje, nustato kvalifikuotų elektroninių požymių liudijimų technines specifikacijas ir standartų referencinius numerius.

45d straipsnis

Požymių tikrinimas pagal autentiškus šaltinius

1. Per 24 mėnesius nuo 6a straipsnio 11 dalyje ir 6c straipsnio 4 dalyje nurodytų įgyvendinimo aktų įsigaliojimo dienos valstybės narės užtikrina, kad bent VI priede išvardytų požymių atveju, kai šie požymiai grindžiami autentiškais viešojo sektoriaus šaltiniais, būtų imtasi priemonių, kad kvalifikuoti elektroninių požymių liudijimų teikėjai naudotojo prašymu galėtų šiuos požymius patikrinti elektroninėmis priemonėmis pagal nacionalinę ar Sąjungos teisę.

2. Per 6 mėnesius nuo šio reglamento įsigaliojimo dienos, atsižvelgdama į atitinkamus tarptautinius standartus, Komisija įgyvendinimo aktu dėl europinių skaitmeninės tapatybės dėklių įgyvendinimo, kaip nurodyta 6a straipsnio 11 dalyje, nustato minimalias technines specifikacijas, standartus ir procedūras, nurodydama požymių katalogus ir požymių liudijimų schemas bei kvalifikuotų elektroninių požymių liudijimų tikrinimo procedūras.

45da straipsnis

Už autentišką šaltinį atsakingos viešojo sektoriaus įstaigos arba jos vardu išduodamam elektroniniam požymių liudijimui keliami reikalavimai

1. Už autentišką šaltinį atsakingos viešojo sektoriaus įstaigos arba jos vardu išduotas elektroninis požymių liudijimas turi atitikti šiuos reikalavimus:

a) VII priede išdėstytus reikalavimus;

b) kvalifikuotame sertifikate, kuriuo tvirtinamas 3 straipsnio 45a dalyje nurodytas viešojo sektoriaus įstaigos, kuri pagal VII priedo b punktą nurodyta kaip leidėja, kvalifikuotas elektroninis parašas arba kvalifikuotas elektroninis spaudas, pateikiamas specialus sertifikuotų požymių rinkinys automatiniam tvarkymui tinkama forma:

i) nurodoma, kad dokumentus išduodanti įstaiga pagal nacionalinę arba Sąjungos teisę įsteigta kaip atsakinga už autentišką šaltinį, kuriuo remiantis išduodamas elektroninis požymių liudijimas, arba kaip įstaiga, paskirta veikti jos vardu;

ii) pateikiamas duomenų rinkinys, kuriame vienareikšmiškai nurodomas i punkte nurodytas autentiškas šaltinis, ir

iii) nurodoma i punkte nurodyta nacionalinė arba Sąjungos teisė.

2. Valstybė narė, kurioje įsteigtos 3 straipsnio 45a dalyje nurodytos viešojo sektoriaus įstaigos, užtikrina, kad elektroninius požymių liudijimus išduodančios viešojo sektoriaus įstaigos būtų tokio paties patikimumo lygio kaip kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai pagal 24 straipsnį.

2a. Valstybės narės praneša Komisijai apie 3 straipsnio 45a dalyje nurodytas viešojo sektoriaus įstaigas. Į šį pranešimą įtraukiama atitikties vertinimo įstaigos parengta atitikties vertinimo ataskaita, kurioje patvirtinama, kad laikomasi šio straipsnio 1, 2 ir 6 dalyse nustatytų reikalavimų. Komisija saugiu ryšių kanalu pateikia visuomenei elektroniniu būdu pasirašytą arba užantspauduotą 3 straipsnio 45a dalyje nurodytų viešojo sektoriaus įstaigų sąrašą automatiniam tvarkymui tinkama forma.

3. Jeigu už autentišką šaltinį atsakingos viešojo sektoriaus įstaigos arba jos vardu išduotas elektroninis požymių liudijimas po pirminio išdavimo panaikinamas, jis netenka galios nuo jo atšaukimo momento. Atšaukus elektroninį liudijimą, jo statuso negalima atkurti.

4. Laikoma, kad elektroninis požymių liudijimas, išduotas už autentišką šaltinį atsakingos viešojo sektoriaus įstaigos arba jos vardu, atitinka šio straipsnio 1 dalyje nustatytus reikalavimus, jei jis atitinka 5 dalyje nurodytus standartus.

5. Per 6 mėnesius nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktu dėl europinių skaitmeninės tapatybės dėklių įgyvendinimo, kaip nurodyta 6a straipsnio 11 dalyje, nustato elektroninio požymių liudijimo, išduoto už autentišką šaltinį atsakingos viešojo sektoriaus įstaigos arba jos vardu, technines specifikacijas ir standartų referencinius numerius.

5a. Per 6 mėnesius nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktu dėl europinių skaitmeninės tapatybės dėklių įgyvendinimo, kaip nurodyta 6a straipsnio 11 dalyje, nustato taikomus formatus, procedūras, specifikacijas ir standartus 2a dalies tikslais.

6. 3 straipsnio 45a dalyje nurodytos viešojo sektoriaus įstaigos, išduodančios elektroninių požymių liudijimus, užtikrina sąsają su europinėmis skaitmeninės tapatybės dėklėmis, išleistomis pagal 6a straipsnį.

45e straipsnis

Europinių skaitmeninės tapatybės dėklių elektroninių požymių liudijimų išdavimas

Kvalifikuotų elektroninių požymių liudijimų teikėjai užtikrina sąsają su europinėmis skaitmeninės tapatybės dėklėmis, pateiktomis pagal 6a straipsnį.

45f straipsnis

Papildomos elektroninio požymių liudijimo paslaugų teikimo taisyklės

1. Kvalifikuoto ir nekvalifikuoto elektroninio požymių liudijimo paslaugų teikėjai nejungia asmens duomenų, susijusių su šių paslaugų teikimu, su asmens duomenimis, gautais iš bet kokių kitų jų ar jų komercinių partnerių siūlomų paslaugų.

2. Su elektroninio požymių liudijimo paslaugų teikimu susiję asmens duomenys saugomi logiškai atskirai nuo kitų duomenų, kuriuos saugo elektroninio požymių liudijimo paslaugų teikėjas.

4. Kvalifikuoto elektroninių požymių liudijimo paslaugų teikėjai taiko funkcinį tokių paslaugų teikimo atskyrimą.

10 SKIRSNIS

ELEKTRONINIO ARCHYVAVIMO PASLAUGOS

45g straipsnis

Elektroninės archyvavimo paslaugos teisinė galia

1. Negalima atsisakyti pripažinti naudojantis elektroninio archyvavimo paslaugomis saugomų elektroninių duomenų teisinės galios ir jų tinkamumo naudoti kaip įrodymą teismo procese tik dėl to, kad jie yra elektroniniai arba kad nėra saugomi naudojantis kvalifikuotomis elektroninio archyvavimo paslaugomis.

2. Kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas taiko elektroninių duomenų, saugomų naudojantis elektroninio archyvavimo paslaugomis, vientisumo ir kilmės prezumpciją visą jų saugojimo laikotarpį.

3. Elektroninio archyvavimo paslauga, teikiama vienoje valstybėje narėje, pripažįstama elektroninio archyvavimo paslauga bet kurioje kitoje valstybėje narėje.

45ga straipsnis

Kvalifikuotoms elektroninio archyvavimo paslaugoms keliami reikalavimai

1. Kvalifikuotos elektroninio archyvavimo paslaugos turi atitikti šiuos reikalavimus:

   a) jas teikia kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai;

   b) jas teikiant naudojamos procedūros ir technologijos, kuriomis pasibaigus technologinio galiojimo laikotarpiui ir bent per visą teisinio ar sutartinio saugojimo laikotarpį galima pratęsti elektroninių duomenų patvarumą ir įskaitomumą, kartu išlaikant jų vientisumą ir kilmę;

c) jas teikiant užtikrinama, kad elektroniniai duomenys būtų saugomi taip, kad būtų apsaugoti nuo praradimo ir pakeitimo, išskyrus jų laikmenos ar elektroninio formato pakeitimus;

d) jas teikiant įgaliotos pasikliaujančiosios šalys gali automatiškai gauti pranešimą, kuriuo patvirtinama, kad iš kvalifikuoto elektroninio archyvo paimtiems elektroniniams duomenims nuo saugojimo laikotarpio pradžios iki paieškos momento taikoma duomenų vientisumo prezumpcija. Šis pranešimas pateikiamas patikimu ir veiksmingu būdu, su kvalifikuotos elektroninio archyvavimo paslaugos teikėjo kvalifikuotu elektroniniu parašu arba kvalifikuotu elektroniniu spaudu.

2. Per 12 mėnesių nuo šio reglamento įsigaliojimo dienos Komisija įgyvendinimo aktais nustato kvalifikuotų elektroninio archyvavimo paslaugų technines specifikacijas ir standartų referencinius numerius. Jeigu kvalifikuotos elektroninio archyvavimo paslaugos atitinka tas specifikacijas ir standartus, laikoma, kad užtikrinta atitiktis kvalifikuotoms elektroninio archyvavimo paslaugoms nustatytiems reikalavimams. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.

11 SKIRSNIS

ELEKTRONINIAI REGISTRAI

45h straipsnis

Elektroninių registrų teisinė galia

1. Negalima atsisakyti pripažinti elektroninio registro teisinės galios ir jo tinkamumo naudoti kaip įrodymo teismo procese tik dėl to, kad jis yra elektroninis arba kad jis neatitinka kvalifikuotų elektroninių registrų reikalavimų.

2. Kvalifikuotame elektroniniame registre saugomiems duomenų įrašams taikoma jų unikalios ir tikslios nuoseklios chronologinės tvarkos ir jų vientisumo prezumpcija.

3. Kvalifikuotas elektroninis registras, esantis vienoje valstybėje narėje, pripažįstamas kvalifikuotu elektroniniu registru bet kurioje kitoje valstybėje narėje.

45i straipsnis

Kvalifikuotiems elektroniniams registrams keliami reikalavimai

1. Kvalifikuoti elektroniniai registrai turi atitikti šiuos reikalavimus:

   a) juos kuria vienas arba daugiau kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų;

   b) juose nustatoma registro duomenų įrašų kilmė;

   c) juose užtikrinama unikali chronologinė duomenų įrašų tvarka;

   d) duomenys juose registruojami taip, kad būtų įmanoma nedelsiant nustatyti bet kokį vėlesnį pakeitimą, visą laiką užtikrinant jų vientisumą.

2. Jeigu elektroninis registras atitinka 3 dalyje nurodytas specifikacijas ir standartus, laikoma, kad užtikrinta atitiktis 1 dalyje nustatytiems reikalavimams.

3. Komisija priima įgyvendinimo aktus, kuriais nustato kvalifikuoto elektroninio registro sukūrimo ir veikimo technines specifikacijas ir standartų referencinius numerius. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

40) įterpiamas 48a straipsnis:

„*48a straipsnis*

Informacijos teikimo reikalavimai

1. Valstybės narės užtikrina, kad būtų renkami europinių skaitmeninės tapatybės dėklių funkcionavimo statistiniai duomenys, kai jie pateikiami jų teritorijoje.

2. Pagal 1 dalį renkami statistiniai duomenys apima šiuos duomenis:

a) galiojančią europinę skaitmeninės tapatybės dėklę turinčių fizinių ir juridinių asmenų skaičių;

b) paslaugų, kurias teikiant pripažįstamos europinės skaitmeninės tapatybės dėklės, tipą ir skaičių;

c) suvestinę ataskaitą, įskaitant duomenis apie incidentus, kuriais užkertamas kelias europinės skaitmeninės tapatybės dėklės naudojimui.

3. 2 dalyje nurodyti statistiniai duomenys viešai skelbiami atviru ir bendrai naudojamu kompiuterio skaitomu formatu.

4. Valstybės narės kasmet ne vėliau kaip kovo 31 d. pateikia Komisijai pagal 2 dalį surinktų statistinių duomenų ataskaitą.“;

41) 49 straipsnis pakeičiamas taip:

„*49 straipsnis*

Peržiūra

1. Komisija atlieka šio reglamento taikymo peržiūrą ir pateikia Europos Parlamentui ir Tarybai ataskaitą per 36 mėnesius nuo jo įsigaliojimo dienos. Komisija visų pirma įvertina 6 ir 6db straipsnių taikymo sritį ir tai, ar tikslinga pakeisti šio reglamento taikymo sritį ar konkrečias jo nuostatas, atsižvelgiant į taikant šį reglamentą įgytą patirtį, taip pat į vartotojų paklausą, technologinius, rinkos ir teisinius pokyčius. Kai būtina, prie tos ataskaitos pridedami pasiūlymai dėl šio reglamento pakeitimų.

2. Vertinimo ataskaita apima europinių skaitmeninės tapatybės dėklių, kurioms taikomas šis reglamentas, prieinamumo ir tinkamumo naudoti vertinimą ir joje įvertinama, ar įpareigojimas pripažinti europines skaitmeninės tapatybės dėkles turi būti nustatytas visiems internetinių privačiųjų paslaugų teikėjams, pasikliaujantiems trečiųjų šalių elektroninės atpažinties paslaugomis naudotojų tapatumui nustatyti.

3. Be to, Komisija kas ketverius metus po pirmoje pastraipoje nurodytos ataskaitos Europos Parlamentui ir Tarybai pateikia pažangos siekiant šio reglamento tikslų ataskaitą.“;

42) 51 straipsnis pakeičiamas taip:

„*51 straipsnis*

Pereinamojo laikotarpio priemonės

1. Pažangūs parašo kūrimo įtaisai, kurių atitiktis buvo nustatyta pagal Direktyvos 1999/93/EB 3 straipsnio 4 dalį, pagal šį reglamentą ir toliau laikomi kvalifikuotais elektroninio parašo kūrimo įtaisais 36 mėnesius nuo šio reglamento įsigaliojimo dienos.

2. Fiziniams asmenims pagal Direktyvą 1999/93/EB išduoti kvalifikuoti sertifikatai pagal šį reglamentą ir toliau laikomi kvalifikuotais elektroninio parašo sertifikatais 24 mėnesius nuo šio reglamento įsigaliojimo dienos.“.

2a. Kai nuotolinio kvalifikuoto elektroninio parašo ir spaudo kūrimo įtaisus administruoja kiti kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai nei nuotolinio kvalifikuoto elektroninio parašo ir spaudo kūrimo įtaisus administruojantys kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai pagal 29a ir 39a straipsnius, 24 mėnesius nuo šio reglamento įsigaliojimo dienos toliau laikoma, kad jiems šioms administravimo paslaugoms teikti nereikia įgyti kvalifikacijos statuso.

2b. Kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai, kuriems iki [iš dalies keičiančio reglamento įsigaliojimo diena] pagal šį reglamentą suteiktas kvalifikacijos statusas, naudodami tapatybės tikrinimo metodus kvalifikuotiems sertifikatams išduoti pagal 24 straipsnio 1 dalį, kuo skubiau, bet ne vėliau kaip per 30 mėnesių nuo iš dalies keičiančio reglamento įsigaliojimo dienos, priežiūros įstaigai pateikia atitikties vertinimo ataskaitą, kurioje įrodo atitiktį 24 straipsnio 1 daliai. Kol bus pateikta tokia atitikties vertinimo ataskaita ir ją įvertins priežiūros įstaiga, kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas gali ir toliau naudotis Reglamento (ES) Nr. 910/2014 24 straipsnio 1 dalyje nustatytais tapatybės tikrinimo metodais.“;

43) I priedas iš dalies keičiamas pagal šio reglamento I priedą;

44) II priedas pakeičiamas šio reglamento II priedo tekstu;

45) III priedas iš dalies keičiamas pagal šio reglamento III priedą;

46) IV priedas iš dalies keičiamas pagal šio reglamento IV priedą;

47) pridedamas naujas V priedas, išdėstytas šio reglamento V priede;

48) prie šio reglamento pridedamas naujas VI priedas.

52 straipsnis

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje

Europos Parlamento vardu	Tarybos vardu
Pirmininkas / Pirmininkė	Pirmininkas / Pirmininkė

I PRIEDAS

I priedo i punktas pakeičiamas taip:

„i) informacija apie kvalifikuoto sertifikato galiojimą arba paslaugos, kuria naudojantis galima gauti tokią informaciją, nuoroda;“.

II PRIEDAS

KVALIFIKUOTIEMS ELEKTRONINIO PARAŠO KŪRIMO ĮTAISAMS KELIAMI REIKALAVIMAI

1. Kvalifikuotais elektroninio parašo kūrimo įtaisai atitinkamomis techninėmis ir procedūrinėmis priemonėmis turi užtikrinti bent tai, kad:

a) būtų tinkamai užtikrintas kuriant elektroninį parašą naudojamų elektroninio parašo kūrimo duomenų konfidencialumas;

b) kuriant elektroninį parašą naudojami elektroninio parašo kūrimo duomenys faktiškai galėtų būti pateikiami tik vieną kartą;

c) būtų pakankamai patikimai panaikinta kuriant elektroninį parašą naudotų elektroninio parašo kūrimo duomenų gavimo galimybė ir kad elektroninis parašas būtų patikimai apsaugotas nuo klastotės taikant šiuo metu turimas technologijas;

d) teisę pasirašyti turintis pasirašantis asmuo galėtų patikimai apsaugoti kuriant elektroninį parašą naudojamus elektroninio parašo kūrimo duomenis taip, kad jais negalėtų pasinaudoti kiti asmenys.

2. Kvalifikuotais elektroninio parašo kūrimo įtaisais nedaroma pasirašomų duomenų pakeitimų ir netrukdoma pateikti šiuos duomenis pasirašančiam asmeniui prieš juos pasirašant.

III PRIEDAS

III priedo i punktas pakeičiamas taip:

„i) informacija apie kvalifikuoto sertifikato galiojimą arba paslaugos, kuria naudojantis galima gauti tokią informaciją, nuoroda;“.

IV PRIEDAS

IV priedo j punktas pakeičiamas taip:

„j) informacija apie kvalifikuoto sertifikato galiojimą arba sertifikato galiojimo būsenos paslaugų, kuriomis naudojantis galima gauti tokią informaciją, nuoroda.“

V PRIEDAS

KVALIFIKUOTŲ ELEKTRONINIŲ POŽYMIŲ LIUDIJIMŲ REIKALAVIMAI

Kvalifikuotuose elektroniniuose požymių liudijimuose turi būti ši informacija:

e) nuoroda, bent automatizuotoms duomenų tvarkymo priemonėms tinkama forma, kad liudijimas išduotas kaip kvalifikuotas elektroninis požymių liudijimas;

f) duomenų rinkinys, kuriuo vienareikšmiškai nurodomas kvalifikuotus elektroninius požymių liudijimus išduodantis kvalifikuotos patikimumo užtikrinimo paslaugos teikėjas, nurodant bent valstybę narę, kurioje jis yra įsisteigęs, ir:

– juridinio asmens atveju: pavadinimas ir, jei taikoma, oficialiame registre nurodytas registracijos numeris,

– fizinio asmens atveju: asmens vardas ir pavardė;

g) duomenų rinkinys, kuriuo vienareikšmiškai nurodomas subjektas, su kuriuo susiję liudijime nurodyti požymiai; jei naudojamas slapyvardis, tai aiškiai nurodoma;

h) liudijamas požymis ar požymiai, įskaitant, jei taikoma, tokių požymių taikymo sričiai nustatyti būtiną informaciją;

i) duomenys apie liudijimo galiojimo laikotarpio pradžią ir pabaigą;

j) liudijimo identifikacinis kodas, kuris turi būti unikalus kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo sistemoje, ir, jei taikoma, turi būti nurodyta liudijimų schema, pagal kurią išduotas požymių liudijimas;

k) liudijimą išduodančio kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo kvalifikuotas elektroninis parašas arba kvalifikuotas elektroninis spaudas;

l) vieta, kurioje galima nemokamai gauti sertifikatą, patvirtinantį g punkte nurodytą kvalifikuotą elektroninį parašą arba kvalifikuotą elektroninį spaudą;

m) informacija apie kvalifikuoto liudijimo galiojimą arba paslaugos, kuria naudojantis galima gauti tokią informaciją, nuoroda.

VI PRIEDAS

BŪTINŲJŲ POŽYMIŲ SĄRAŠAS

Be to, kas nustatyta 45d straipsnyje, valstybės narės užtikrina, kad būtų imamasi priemonių sudaryti sąlygas kvalifikuotiems elektroninių požymių liudijimų teikėjams elektroniniu būdu naudotojui prašant patikrinti šių požymių tikrumą pagal atitinkamą autentišką šaltinį nacionaliniu lygmeniu ar per paskirtus nacionaliniu lygmeniu pripažįstamus tarpininkus laikantis nacionalinės ar Sąjungos teisės ir tais atvejais, kai šie požymiai grindžiami viešojo sektoriaus autentiškais šaltiniais:

1. adreso;
2. amžiaus;
3. lyties;
4. civilinės būklės;
5. šeimos sudėties;
6. pilietybės / tautybės;
7. mokslo kvalifikacijų, pareigų ir licencijų;
8. profesinių kvalifikacijų, pareigų ir licencijų;
9. viešųjų leidimų ir licencijų;
10. finansinių ir įmonės duomenų.

VII PRIEDAS

UŽ AUTENTIŠKĄ ŠALTINĮ ATSAKINGOS VIEŠOSIOS ĮSTAIGOS ARBA JOS VARDU IŠDUOTIEMS ELEKTRONINIAMS POŽYMIŲ LIUDIJIMAMS KELIAMI REIKALAVIMAI

Už autentišką šaltinį atsakingos viešosios įstaigos arba jos vardu išduotame elektroniniame požymių liudijime pateikiama:

a) nuoroda, bent automatiniam tvarkymui tinkama forma, kad liudijimas buvo išduotas kaip už autentišką šaltinį atsakingos viešosios įstaigos arba jos vardu išduodamas elektroninis požymių liudijimas;
b) duomenų rinkinys, kuriuo vienareikšmiškai nurodoma elektroninį požymių liudijimą išdavusi viešoji įstaiga, įskaitant bent valstybę narę, kurioje ta viešoji įstaiga yra įsteigta, tos įstaigos pavadinimą ir, kai taikytina, registracijos numerį, kaip nurodyta oficialiuose įrašuose;
c) duomenų rinkinys, kuriuo vienareikšmiškai nurodomas subjektas, su kuriuo susiję liudijime nurodyti požymiai; jei naudojamas slapyvardis, tai aiškiai nurodoma;
d) liudijamas požymis ar požymiai, įskaitant, jei taikoma, tokių požymių taikymo sričiai nustatyti būtiną informaciją;
e) duomenys apie liudijimo galiojimo laikotarpio pradžią ir pabaigą;
f) liudijimo identifikacinis kodas, kuris turi būti unikalus išduodančios viešosios įstaigos sistemoje, ir, jei taikoma, turi būti nurodyta liudijimų schema, pagal kurią išduotas požymių liudijimas;
g) išduodančios įstaigos kvalifikuotas elektroninis parašas arba kvalifikuotas elektroninis spaudas;
h) vieta, kurioje galima nemokamai gauti sertifikatą, patvirtinantį g punkte nurodytą kvalifikuotą elektroninį parašą arba kvalifikuotą elektroninį spaudą;
i) informacija apie liudijimo galiojimą arba paslaugos, kuria naudojantis galima gauti tokią informaciją, nuoroda.

_____