

**EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS (ES) Nr. 910/2014****2014 m. liepos 23 d.****dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB**

EUROPOS PARLAMENTAS IR EUROPOS SAJUNGOS 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 <sup>(1)</sup>,

laikydami įprastos teisėkūros procedūros <sup>(2)</sup>,

kadangi:

- (1) pasitikėjimo internetine aplinka skatinimas yra svarbus ekonominės ir socialinės plėtros veiksnys. Trūkstant pasitikėjimo, ypač dėl pastebimo teisinio tikrumo trūkumo, vartotojai, įmonės ir viešosios valdžios institucijos vengia vykdyti operacijas elektroniniu būdu ir pradėti naudotis naujomis paslaugomis;
- (2) šiuo reglamentu siekiama stiprinti pasitikėjimą elektroninėmis operacijomis vidaus rinkoje, suteikiant bendrą pagrindą saugiai vykdyti elektronines piliečių, verslo ir viešosios valdžios institucijų tarpusavio operacijas, taip didinant viešųjų ir privačiųjų internetinių paslaugų, elektroninio verslo ir elektroninės prekybos veiksmingumą Sąjungoje;
- (3) Europos Parlamento ir Tarybos direktyva 1999/93/EB <sup>(3)</sup> iš esmės buvo skirta tik elektroniniams parašams, nenustatant išsamios tarpvalstybinės ir tarpšakinės sistemos, kuria būtų užtikrintos saugios, patikimos ir patogios naudoti elektroninės operacijos. Šiuo reglamentu patobulinamas ir išplečiamas tos direktyvos *acquis*;
- (4) 2010 m. rugpjūčio 26 d. Komisijos komunikate „Europos skaitmeninė darbotvarkė“ nurodyta, kad skaitmeninės rinkos susiskaidymas, sąveikumo stoka ir elektroninių nusikaltimų gausėjimas yra pagrindinės sėkmingo skaitmeninės ekonomikos ciklo užtikrinimo kliūtys. 2010 m. ES pilietybės ataskaitoje „Kliūčių ES piliečių teisėms šalinimas“ Komisija dar kartą pabrėžė poreikį spręsti pagrindines problemas, trukdančias Sąjungos piliečiams naudotis bendrosios skaitmeninės rinkos ir tarpvalstybinių skaitmeninių paslaugų teikiamais privalumais;
- (5) 2011 m. vasario 4 d. ir 2011 m. spalio 23 d. išvadose Europos Vadovų Taryba paprašė Komisijos ne vėliau kaip 2015 m. sukurti bendrąją skaitmeninę rinką, kad, sudarant palankesnes sąlygas tarpvalstybiniu mastu naudotis internetinėmis paslaugomis ypač daug dėmesio skiriant saugios elektroninės atpažinties ir tapatumo nustatymo palengvinimui, būtų galima daryti sparčią pažangą pagrindinėse skaitmeninės ekonomikos srityse ir skatinti visiškai integruotos bendrosios skaitmeninės rinkos kūrimąsi;

<sup>(1)</sup> OL C 351, 2012 11 15, p. 73.

<sup>(2)</sup> 2014 m. balandžio 3 d. Europos Parlamento pozicija (dar nepaskelbta Oficialiajame leidinyje) ir 2014 m. liepos 23 d. Tarybos sprendimas.

<sup>(3)</sup> 1999 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyva 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos (OL L 13, 2000 1 19, p. 12).

- (6) 2011 m. gegužės 27 d. išvadose Taryba ragino Komisiją prisidėti prie bendrosios skaitmeninės rinkos kūrimo nustatant tinkamas pagrindinių priemonių, kaip antai elektroninės atpažinties, elektroninių dokumentų, elektroninių parašų ir elektroninio pristatymo paslaugų, abipusio tarpvalstybinio pripažinimo ir sąveikių e. valdžios paslaugų teikimo visoje Europos Sąjungoje sąlygas;
- (7) 2010 m. rugsėjo 21 d. rezoliucijoje dėl elektroninės prekybos vidaus rinkos užbaigimo <sup>(1)</sup> Europos Parlamentas pabrėžė, kad svarbu užtikrinti elektroninių paslaugų, ypač elektroninių parašų, saugumą, ir kad Europos lygiu būtina sukurti pamatinę viešąją infrastruktūrą, bei paprašė Komisijos sukurti Europos tinkamumo patvirtinimo institucijų portalą, siekiant užtikrinti tarpvalstybinį elektroninių parašų sąveikumą ir padidinti internetu sudarytų sandorių saugumą;
- (8) Europos Parlamento ir Tarybos direktyva 2006/123/EB <sup>(2)</sup> reikalaujama, kad valstybės narės įsteigtų „kontaktinius centrus“ (toliau – KC) siekiant užtikrinti, jog būtų galima lengvai, nuotoliniu būdu, elektroninėmis priemonėmis per atitinkamą kontaktinį centrą susisiekti su reikiamomis valdžios institucijomis, atlikti visas procedūras ir formalumus, susijusius su teise teikti paslaugas ir ja naudotis. Daugeliui internetinių paslaugų, teikiamų per KC, reikalinga elektroninė atpažintis, tapatumo nustatymas ir parašas;
- (9) daugeliu atveju piliečiai negali pasinaudoti savo elektroninės atpažinties priemonėmis, kad jų tapatybė būtų nustatyta kitoje valstybėje narėje, nes jų šalyje taikomos nacionalinės elektroninės atpažinties schemas kitose valstybėse narėse nepripažįstamos. Ta elektroninė kliūtis trukdo paslaugų teikėjams pasinaudoti visais vidaus rinkos privalumais. Abipusiu pagrindu pripažintos elektroninės atpažinties priemonės palengvins tarpvalstybinį įvairių paslaugų teikimą vidaus rinkoje ir suteiks įmonėms galimybę vykdyti veiklą tarpvalstybiniu pagrindu, išvengiant daugelio problemų, kylančių santykiuose su viešosios valdžios institucijomis;
- (10) Europos Parlamento ir Tarybos direktyva 2011/24/ES <sup>(3)</sup> įsteigtas už e. sveikatą atsakingų nacionalinės valdžios institucijų tinklas. Siekiant pagerinti tarpvalstybinių sveikatos priežiūros paslaugų saugumą ir tęstinumą, reikalaujama, kad šis tinklas parengtų tarpvalstybinio prisijungimo prie elektroninių sveikatos priežiūros duomenų ir paslaugų gaires, įskaitant padėtų rengti „bendras identifikavimo ir autentifikavimo priemones, kad būtų sudarytos palankesnės sąlygos perduoti duomenis teikiant tarpvalstybines sveikatos priežiūros paslaugas“. Abipusis elektroninės atpažinties ir tapatumo nustatymo priemonių pripažinimas yra labai svarbus Europos piliečių tarpvalstybinės sveikatos priežiūros faktinio užtikrinimo veiksnys. Kai žmonės keliauja gydymosi tikslais, jų medicininiai duomenys turi būti prieinami jų gydymosi šalyje. Tam būtina vientisa, saugi ir patikima elektroninės atpažinties sistema;
- (11) šis reglamentas turėtų būti taikomas visiškai laikantis asmens duomenų apsaugos principų, numatytų Europos Parlamento ir Tarybos direktyvoje 95/46/EB <sup>(4)</sup>. Šiuo klausimu, atsižvelgiant į šiuo reglamentu nustatytą abipusio pripažinimo principą, internetinės paslaugos tapatumo nustatymas turėtų būti susijęs tik su tų atpažinties duomenų, kurie yra adekvatūs, susiję ir nepertekliniai tam, kad būtų galima pasinaudoti ta internetine paslauga, tvarkymu. Be to, patikimumo užtikrinimo paslaugų teikėjai ir priežiūros įstaigos turėtų laikytis Direktyvos 95/46/EB reikalavimų, susijusių su konfidencialumu ir duomenų tvarkymo saugumu;
- (12) vienas šio reglamento uždavinių – pašalinti esamas valstybėse narėse naudojamų elektroninės atpažinties priemonių, reikalingų norint nustatyti tapatybę bent siekiant pasinaudoti viešosiomis paslaugomis, tarpvalstybinio naudojimo kliūtis. Šiuo reglamentu nesiekama kištis į valstybėse narėse įdiegtų elektroninės atpažinties valdymo sistemas ir su jomis susijusias infrastruktūras. Šio reglamento tikslas – užtikrinti, kad naudojantis valstybių narių siūlomomis tarpvalstybinėmis internetinėmis paslaugomis būtų galima užtikrinti saugią elektroninę atpažintį ir tapatumo nustatymą;

<sup>(1)</sup> OL C 50 E, 2012 2 21, p. 1.

<sup>(2)</sup> 2006 m. gruodžio 12 d. Europos Parlamento ir Tarybos direktyva 2006/123/EB dėl paslaugų vidaus rinkoje (OL L 376, 2006 12 27, p. 36).

<sup>(3)</sup> 2011 m. kovo 9 d. Europos Parlamento ir Tarybos direktyva 2011/24/ES dėl pacientų teisių į tarpvalstybines sveikatos priežiūros paslaugas įgyvendinimo (OL L 88, 2011 4 4, p. 45).

<sup>(4)</sup> 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (OL L 281, 1995 11 23, p. 31).

- (13) valstybėms narėms turėtų būti palikta laisvė elektroninės atpažinties tikslais naudoti arba diegti priemones, reikalingas norint pasinaudoti internetinėmis paslaugomis. Be to, joms turėtų būti suteikta galimybė spręsti, ar į tų priemonių užtikrinimą įtraukti privatųjį sektorių. Valstybės narės neturėtų būti įpareigojamos pranešti Komisijai apie savo elektroninės atpažinties schemas. Valstybės narės turėtų pačios spręsti, ar pranešti Komisijai apie visas elektroninės atpažinties schemas, nacionaliniu lygiu taikomas tam, kad būtų galima pasinaudoti bent viešosiomis internetinėmis paslaugomis arba tam tikromis paslaugomis, ar pranešti tik apie kai kurias schemas, ar visai apie jas nepranešti;
- (14) šiame reglamente turi būti nustatytos tam tikros sąlygos, numatančios, kurios elektroninės atpažinties priemonės turi būti pripažįstamos ir koku būdu turėtų būti pranešama apie elektroninės atpažinties schemas. Tos sąlygos turėtų padėti valstybėms narėms įgyti būtiną pasitikėjimą viena kitos elektroninės atpažinties schemomis ir abipusiai pripažinti elektroninės atpažinties priemones, kurioms taikomos schemas, apie kurias pranešta. Abipusio pripažinimo principas turėtų būti taikomas, jeigu pranešančiosios valstybės narės elektroninės atpažinties schema laikomasi pranešimo sąlygų ir jeigu pranešimas buvo paskelbtas *Europos Sąjungos oficialiajame leidinyje*. Vis dėlto abipusio pripažinimo principas turėtų būti susijęs tik su internetinės paslaugos tapatumo nustatymu. Galimybė naudotis tomis internetinėmis paslaugomis ir galutinis jų suteikimas prašytojui turėtų būti glaudžiai susieti su teise gauti tokias paslaugas nacionalinės teisės aktuose nustatytais sąlygomis;
- (15) pareiga pripažinti elektroninės atpažinties priemones turėtų būti susijusi tik su tomis priemonėmis, kurių tapatybės saugumo užtikrinimo lygis atitinka arba yra aukštesnis už lygį, kurio reikalaujama norint pasinaudoti ta konkrečia internetine paslauga. Be to, ta pareiga turėtų būti taikoma tik tuomet, kai konkreti viešojo sektoriaus įstaiga taiko pakankamą arba aukštą saugumo užtikrinimo lygį norint pasinaudoti ta internetine paslauga. Pagal Sąjungos teisę valstybės narės turėtų galėti pasirinkti, ar pripažinti elektroninės atpažinties priemones, kurių tapatybės saugumo užtikrinimo lygis yra žemesnis;
- (16) saugumo užtikrinimo lygiais turėtų būti apibūdinamas elektroninės atpažinties priemonės patikimumo laipsnis nustatant asmens tapatybę ir taip užtikrinant, kad asmuo, kuris pareiškia turintis tam tikrą tapatybę iš tiesų yra asmuo, kuriam ta tapatybė buvo priskirta. Saugumo užtikrinimo lygis priklauso nuo pareikštos arba patvirtintos asmens tapatybės patikimumo laipsnio, kuris nurodomas elektroninės atpažinties priemonėmis, atsižvelgiant į procesus (pavyzdžiui, tapatybės įrodymą ir patikrinimą bei tapatumo nustatymą), valdymo veiklą (pavyzdžiui, elektroninės atpažinties priemones išduodantį subjektą ir tokių priemonių išdavimo tvarką) ir įgyvendintas techninės kontrolės priemones. Vykdant Sąjungos finansuojamus didelio masto bandomuosius projektus, standartizaciją ir tarptautinę veiklą nustatyta įvairių saugumo užtikrinimo lygių techninių reikalavimų ir aprašymų. Visų pirma didelio masto bandomajame projekte STORK ir ISO 29115 nurodomi, *inter alia*, 2, 3 ir 4 lygiai, į kuriuos reikėtų kuo labiau atsižvelgti nustatant minimalius techninius reikalavimus, standartus ir procedūras, taikomus žemam, pakankamam ir aukštam saugumo užtikrinimo lygiams, kaip apibrėžta šiame reglamente, siekiant užtikrinti nuoseklų šio reglamento taikymą, visų pirma aukšto saugumo užtikrinimo lygio, susijusio su tapatybės identifikavimu siekiant išduoti kvalifikuotus sertifikatus, atžvilgiu. Nustatyti reikalavimai turėtų būti technologiniu požiūriu neutralūs. Turėtų būti įmanoma įvykdyti būtinus saugumo reikalavimus taikant skirtingas technologijas;
- (17) valstybės narės turėtų skatinti privatųjį sektorių atpažinties tikslais savanoriškai naudoti elektroninės atpažinties priemones pagal schemą, apie kurią pranešta, kai to reikia norint pasinaudoti internetinėmis paslaugomis arba atlikti elektronines operacijas. Galimybė naudoti tokias elektroninės atpažinties priemones leistų privačiam sektoriui pasikliauti elektronine atpažintimi ir tapatumo nustatymu, kurie jau plačiai taikomi daugumoje valstybių narių bent viešųjų paslaugų tikslais, ir sudaryti įmonėms bei piliečiams palankesnes sąlygas tarpvalstybiniu mastu naudotis tų valstybių narių teikiamomis internetinėmis paslaugomis. Kad privačiam sektoriui būtų lengviau naudoti tokias elektroninės atpažinties priemones tarpvalstybiniu mastu, privačiojo sektoriaus pasikliaujančiosioms šalims, kurios įsteigtos ne tos valstybės narės teritorijoje, turėtų būti sudarytos sąlygos naudotis bet kurios valstybės narės teikiama tapatumo nustatymo galimybe tokiomis pačiomis sąlygomis, kurios taikomos toje valstybėje narėje įsteigtoms privačiojo sektoriaus pasikliaujančiosioms šalims. Todėl pranešančioji valstybė narė privačiojo sektoriaus pasikliaujančiosioms šalims gali nustatyti naudojimosi tapatumo nustatymo priemonėmis sąlygas. Tokiose naudojimosi sąlygose gali būti pateikiama informacija, ar privačiojo sektoriaus pasikliaujančiosios šalys šiuo metu turi galimybę naudotis tapatumo nustatymo priemone, susijusia su schema, apie kurią pranešta;
- (18) šiuo reglamentu turėtų būti numatoma pranešančiosios valstybės narės, elektroninės atpažinties priemonę išduodančios šalies ir tapatumo nustatymo procedūrą vykdančios šalies atsakomybė už atitinkamų pareigų pagal šį reglamentą nevykdymą. Tačiau šis reglamentas turėtų būti taikomas laikantis nacionalinių atsakomybę reglamentuojančių taisyklių. Todėl jis neturi poveikio toms nacionalinėms taisyklėms, pavyzdžiui, dėl žalos apibrėžties arba dėl atitinkamų taikytinų procedūrinių taisyklių, įskaitant dėl įrodinėjimo pareigos.

- (19) elektroninių atpažinties schemų saugumas itin svarbus patikimam tarpvalstybiniam elektroninių atpažinties priemonių abipusiam pripažinimui. Atsižvelgdamos į tai, valstybės narės Sąjungos lygiu turėtų bendradarbiauti elektroninių atpažinties schemų saugumo ir sąveikumo užtikrinimo srityje. Jeigu tam, kad pasikliaujančiosios šalys nacionaliniu lygiu galėtų naudotis elektroninėmis atpažinties schemomis, reikalingos specialios aparatinės ar programinės įrangos, laikantis tarpvalstybinio sąveikumo principo tos valstybės narės ne jų teritorijoje įsteigtoms pasikliaujančiosioms šalims neturėtų nustatyti tokių reikalavimų ir susijusių sąnaudų. Tuo atveju reikėtų aptarti ir rasti tinkamus sprendimo būdus, neviršijant sąveikumo sistemos apimties. Nepaisant to, techniniai reikalavimai, susiję su nacionalinių elektroninių atpažinties priemonių konkrečiomis specifikacijomis, kurie, kaip tikėtina, turės poveikį tokių elektroninių priemonių (pvz., lustinių kortelių) turėtojams, yra neišvengiami;
- (20) valstybių narių bendradarbiavimas turėtų padėti užtikrinti elektroninės atpažinties schemų, apie kurias pranešta, techninį sąveikumą, siekiant aukšto lygio pasitikėjimo ir rizikos lygį atitinkančio saugumo. Tokį bendradarbiavimą turėtų palengvinti valstybių narių keitimasis informacija ir geriausia praktika, siekiant užtikrinti abipusį pripažinimą;
- (21) šiuo reglamentu taip pat turėtų būti nustatyta bendroji teisinė patikimumo užtikrinimo paslaugų naudojimo sistema. Vis dėlto juo neturėtų būti nustatyta bendra pareiga naudotis šiomis paslaugomis arba įdiegti prieigos tašką visoms esamoms patikimumo užtikrinimo paslaugoms. Visų pirma juo neturėtų būti reglamentuojamas paslaugų, kuriomis naudojamosi tik uždaroje sistemoje tarp apibrėžtos grupės dalyvių ir kurios neturi poveikio trečiosioms šalims, teikimas. Pavyzdžiui, šio reglamento reikalavimai neturėtų būti taikomi sistemoms, sukurtoms versle arba viešojo valdymo institucijose siekiant valdyti vidaus procedūras, kuriose naudojamosi patikimumo užtikrinimo paslaugomis. Tik visuomenei teikiamos patikimumo užtikrinimo paslaugos, kurios turi poveikio trečiosioms šalims, turėtų atitikti šiame reglamente nustatytus reikalavimus. Šiuo reglamentu neturėtų būti reglamentuojami ir aspektai, susiję su sutarčių sudarymu arba kitų teisinių pareigų nustatymu ir šių sutarčių bei pareigų galiojimu, kai yra nacionalinės arba Sąjungos teisės aktais nustatytų reikalavimų dėl formos. Be to, juo nedaromas poveikis nacionalinės formos reikalavimams, susijusiems su viešaisiais registrais, visų pirma, komerciniais ir žemės registrais;
- (22) siekiant paskatinti jų bendrą tarpvalstybinį naudojimą, patikimumo užtikrinimo paslaugas turėtų būti galima naudoti kaip įrodymus visų valstybių narių teismo procesuose. Patikimumo užtikrinimo paslaugų teisinė galia turi būti reglamentuojama nacionalinės teisės aktuose, išskyrus atvejus, jei šiame reglamente būtų numatyta kitaip;
- (23) tiek, kiek šiuo reglamentu nustatoma pareiga pripažinti patikimumo užtikrinimo paslaugą, tokia patikimumo užtikrinimo paslauga gali būti atmesta tik tuo atveju, jeigu asmuo, kuriam skirta pareiga dėl techninių priežasčių, kurios tiesiogiai nuo jo nepriklauso, negali jos perskaityti arba patikrinti. Vis dėlto dėl tos pareigos viešoji įstaiga savaime neprivalo įsigyti aparatinės ar programinės įrangos, būtinos visų esamų patikimumo užtikrinimo paslaugų techniniam nuskaitymui;
- (24) valstybės narės gali palikti galioti arba nustatyti Sąjungos teisę atitinkančias nacionalines nuostatas, susijusias su patikimumo užtikrinimo paslaugomis tiek, kiek tos paslaugos nėra visiškai suderintos pagal šį reglamentą. Vis dėlto šį reglamentą atitinkančios patikimumo užtikrinimo paslaugos turėtų būti laisvai platinamos vidaus rinkoje;
- (25) valstybėms narėms turėtų būti palikta laisvė apibrėžti kitas, į šiame reglamente numatytą galutinį patikimumo užtikrinimo paslaugų sąrašą neįtrauktas patikimumo užtikrinimo paslaugas, kad jos nacionaliniu mastu būtų pripažįstamos kaip kvalifikuotos patikimumo užtikrinimo paslaugos;
- (26) atsižvelgiant į technologijų pažangos tempą, šiame reglamente turėtų būti įtvirtintas palankumo naujovių diegimui principas;
- (27) šis reglamentas turėtų būti neutralus technologiniu požiūriu. Šiuo reglamentu suteiktas teisinis galias turėtų būti galima įgyvendinti bet kokiomis techninėmis priemonėmis, atitinkančiomis šio reglamento reikalavimus;

- (28) siekiant sustiprinti visų pirma mažųjų ir vidutinių įmonių (toliau – MVI) bei vartotojų pasitikėjimą vidaus rinka ir paskatinti patikimumo užtikrinimo paslaugų ir produktų naudojimą, turėtų būti įvestos naujos – kvalifikuotų patikimumo užtikrinimo paslaugų ir kvalifikuotų patikimumo užtikrinimo paslaugų teikėjo – sąvokos, kad būtų galima nurodyti reikalavimus ir pareigas, kuriais būtų užtikrintas aukštas bet kokių naudojamų arba teikiamų kvalifikuotų patikimumo užtikrinimo paslaugų ir produktų saugumo lygis;
- (29) atsižvelgiant į pareigas, nustatytas pagal Jungtinių Tautų neigaliųjų teisių konvenciją, patvirtintą Tarybos sprendimu 2010/48/EB <sup>(1)</sup>, ypač pagal Konvencijos 9 straipsnį, neigalieji turėtų galėti vienodomis sąlygomis, kaip ir vartotojai, naudotis patikimumo užtikrinimo paslaugomis ir galutinio vartojimo produktais, naudojamais teikiant tas paslaugas. Todėl, jeigu įmanoma, neigaliesiems turėtų būti sudaroma galimybė naudotis teikiamomis patikimumo užtikrinimo paslaugomis ir teikiant tas paslaugas naudojamais galutinio vartojimo produktais. Atliekant įgyvendinamumo vertinimą, *inter alia*, turėtų būti vertinami techniniai ir ekonominiai aspektai;
- (30) valstybės narės turėtų paskirti priežiūros įstaigą ar įstaigas, kad jos vykdytų priežiūros veiklą pagal šį reglamentą. Be to, valstybės narės turėtų galėti nuspręsti, abipusiu pagrindu susitarusios su kita valstybe nare, paskirti priežiūros įstaigą tos kitos valstybės narės teritorijoje;
- (31) priežiūros įstaigos turėtų bendradarbiauti su duomenų apsaugos institucijomis, pavyzdžiui, informuodamos jas apie kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų audito rezultatus tais atvejais, kai tikėtina, kad buvo pažeistos asmens duomenų apsaugos taisyklės. Informacija visų pirma turėtų būti teikiama apie saugumo incidentus ir asmens duomenų naudojimo pažeidimus;
- (32) visi patikimumo užtikrinimo paslaugų teikėjai turėtų vadovautis gerąja saugumo praktika, atitinkančia su jų veikla susijusią riziką, kad būtų sustiprintas vartotojų pasitikėjimas bendrąja rinka;
- (33) nuostatomis dėl slapyvardžių naudojimo sertifikatuose neturėtų būti kliudoma valstybėms narėms reikalauti nustatyti asmenų tapatybę pagal Sąjungos arba nacionalinės teisės aktus;
- (34) siekiant užtikrinti panašų kvalifikuotų patikimumo užtikrinimo paslaugų saugumo lygį, visos valstybės narės turėtų laikytis bendrų esminių priežiūros reikalavimų. Kad tuos reikalavimus būtų lengviau nuosekliai taikyti visoje Sąjungoje, valstybės narės turėtų patvirtinti palyginamas procedūras ir keistis informacija apie savo vykdomą priežiūros veiklą bei geriausia praktika šioje srityje;
- (35) šiame reglamente nustatyti reikalavimai, visų pirma reikalavimai dėl saugumo ir atsakomybės, turėtų būti taikomi visiems patikimumo užtikrinimo paslaugų teikėjams, siekiant užtikrinti deramą stropumą, skaidrumą ir atskaitomybę jiems atliekant savo veiklą ir teikiant paslaugas. Vis dėlto, atsižvelgiant į patikimumo užtikrinimo paslaugų teikėjų teikiamų paslaugų rūšį, tikslinga tų reikalavimų atžvilgiu atskirti kvalifikuotus ir nekvalifikuotus patikimumo užtikrinimo paslaugų teikėjus;
- (36) nustatčius priežiūros režimą visiems patikimumo užtikrinimo paslaugų teikėjams būtų užtikrintos vienodos sąlygos jų atliekamos veiklos ir teikiamų paslaugų saugumo ir atskaitomybės atžvilgiu, taip prisidedant prie vartotojų apsaugos ir vidaus rinkos veikimo. Nekvalifikuotiems patikimumo užtikrinimo paslaugų teikėjams turėtų būti taikoma negriežta ir pasyvi *ex-post* priežiūra, grindžiama jų teikiamų paslaugų ir atliekamos veiklos pobūdžiu. Todėl priežiūros įstaiga neturėtų turėti bendros pareigos prižiūrėti nekvalifikuotus paslaugų teikėjus. Priežiūros įstaiga turėtų imtis veiksmų tik tuomet, kai yra informuojama (pavyzdžiui, paties nekvalifikuoto paslaugų teikėjo, kitos priežiūros įstaigos, vartotojo ar verslo partnerio pranešimu arba atlikusi tyrimą), kad nekvalifikuotas patikimumo užtikrinimo paslaugų teikėjas nesilaiko šio reglamento reikalavimų;

<sup>(1)</sup> 2009 m. lapkričio 26 d. Tarybos sprendimas 2010/48/EB dėl Jungtinių Tautų neigaliųjų teisių konvencijos sudarymo Europos bendrijos vardu (OL L 23, 2010 1 27, p. 35).



- (37) šiuo reglamentu turėtų būti numatoma visų patikimumo užtikrinimo paslaugų teikėjų atsakomybė. Visų pirma, juo nustatomas atsakomybės režimas, pagal kurį visi patikimumo užtikrinimo paslaugų teikėjai turėtų būti atsakingi už žalą, kurią patyrė fizinis ar juridinis asmuo, nes nebuvo laikomasi šiame reglamente numatyty pareigų. Siekiant palengvinti finansinės rizikos, kurią gali patirti patikimumo užtikrinimo paslaugų teikėjai arba dėl kurios jie turėtų apsidrausti, įvertinimą, šiuo reglamentu patikimumo užtikrinimo paslaugų teikėjams leidžiama tam tikromis sąlygomis nustatyti naudojimosi savo teikiamomis paslaugomis ribas ir nebūti atsakingiems už žalą, patirtą dėl to, kad buvo naudojamos tuos apribojimus viršijančiomis paslaugomis. Klientai turėtų būti tinkamai iš anksto informuoti apie apribojimus. Trečioji šalis turėtų atpažinti tuos apribojimus, pavyzdžiui, įtraukiant informaciją apie tuos apribojimus į teikiamos paslaugos sąlygas arba kitais atpažįstamais būdais. Norint, kad tie principai galėtų, šis reglamentas turėtų būti taikomas laikantis nacionalinių atsakomybę reglamentuojančių taisyklių. Todėl šiuo reglamentu nedaromas poveikis nacionalinėms taisyklėms, pavyzdžiui, reglamentuojančioms žalos apibrėžti, tyčią, neat-sargumą ar atitinkamas taikomas procedūrinės taisyklės;
- (38) siekiant suinteresuotosioms šalims suteikti tinkamos informacijos saugumo ar vientisumo pažeidimo atveju, labai svarbu, kad būtų pranešama apie saugumo pažeidimus ir kad būtų atliekami saugumo rizikos vertinimai;
- (39) kad Komisija ir valstybės narės galėtų įvertinti šiuo reglamentu sukurto pranešimų apie pažeidimus mechanizmo veiksmingumą, turėtų būti reikalaujama, kad priežiūros įstaigos teiktų Komisijai ir Europos Sąjungos tinklų ir informacijos apsaugos agentūrai (ENISA) informacijos suvestines;
- (40) kad Komisija ir valstybės narės galėtų įvertinti šiuo reglamentu nustatyto geresnės priežiūros mechanizmo veiksmingumą, turėtų būti reikalaujama, kad priežiūros įstaigos teiktų ataskaitas apie savo veiklą. Tai padėtų palengvinti priežiūros įstaigų keitimąsi gerąja praktika ir užtikrintų patikrą, ar esminiai priežiūros reikalavimai visose valstybėse narėse yra įgyvendinami nuosekliai ir veiksmingai;
- (41) kad būtų užtikrintas kvalifikuotų patikimumo užtikrinimo paslaugų tvarumas ir pastovumas bei sustiprintas vartotojų pasitikėjimas kvalifikuotų patikimumo užtikrinimo paslaugų tęstinumu, priežiūros įstaigos turėtų patikrinti, ar tais atvejais, kai kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai nutraukia veiklą, parengtos nutraukimo planų nuostatos ir ar jos teisingai taikomos;
- (42) siekiant palengvinti kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų priežiūrą, pavyzdžiui, kai teikėjas teikia paslaugas kitos valstybės narės teritorijoje ir joje jam netaikoma priežiūra arba kai paslaugos teikėjo kompiuteriai yra kitos nei jo įsisteigimo valstybės narės teritorijoje, turėtų būti nustatyta valstybių narių priežiūros įstaigų savitarpio pagalbos sistema;
- (43) siekiant užtikrinti, kad kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai ir jų teikiamos paslaugos atitiktų šiame reglamente nustatytus reikalavimus, atitikties vertinimus turėtų atlikti atitikties vertinimo įstaiga, o po to parengtas atitikties įvertinimo ataskaitas kvalifikuotų patikimumo užtikrinimo paslaugų teikėjai turėtų pateikti priežiūros įstaigai. Kiekvieną kartą reikalaujama, kad kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas pateiktų *ad hoc* atitikties vertinimo ataskaitą, priežiūros įstaiga turėtų visų pirma laikytis gero administravimo principų, įskaitant pareigą pagrįsti savo sprendimus, taip pat laikytis proporcingumo principo. Todėl priežiūros įstaiga turėtų deramai pagrįsti sprendimą reikalauti *ad hoc* atitikties vertinimo;
- (44) šiuo reglamentu siekiama užtikrinti nuoseklią sistemą, kad būtų pasiektas aukštas patikimumo užtikrinimo paslaugų apsaugos ir teisinio tikrumo lygis. Šiuo požiūriu Komisija, spręsdama produktų ir paslaugų atitikties vertinimo klausimus, turėtų, jei taikytina, ieškoti sąveikos su šiuo metu taikomais susijusiais Europos ir tarptautiniais modeliais, kaip antai Europos Parlamento ir Tarybos reglamentu (EB) Nr. 765/2008 <sup>(1)</sup>, kuriuo nustatomi atitikties vertinimo įstaigų akreditavimo ir produktų rinkos priežiūros reikalavimai;

(<sup>1</sup>) 2008 m. liepos 9 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 765/2008, nustatantis su gaminių prekyba susijusius akreditavimo ir rinkos priežiūros reikalavimus ir panaikinantys Reglamentą (EEB) Nr. 339/93 (OL L 218, 2008 8 13, p. 30).

- (45) kad būtų galima užtikrinti veiksmingą inicijavimo procesą, kuriuo kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai ir jų teikiamos kvalifikuotos patikimumo užtikrinimo paslaugos turėtų būti įtraukiami į patikimumo sąrašus, turėtų būti paskatintas numatomų kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų ir kompetentingos priežiūros įstaigos preliminarus bendravimas, siekiant sudaryti palankesnes sąlygas deramam stropumui, kuris būtinas teikiant kvalifikuotas patikimumo užtikrinimo paslaugas;
- (46) patikimi sąrašai yra labai svarbūs tam, kad būtų įgyjamas rinkos dalyvių tarpusavio pasitikėjimas, nes juose, atliekant priežiūrą, nurodomas paslaugos teikėjo kvalifikacijos statusas;
- (47) pasitikėjimas internetinėmis paslaugomis ir tų paslaugų patogumas yra būtini, kad naudotojai galėtų visapusiškai naudotis ir sąmoningai pasitikėti elektroninėmis paslaugomis. Šiuo tikslu turėtų būti sukurtas ES pasitikėjimo ženklas, kad būtų galima atpažinti kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų teikiamas kvalifikuotas patikimumo užtikrinimo paslaugas. Tokiu ES pasitikėjimo ženklu kvalifikuotos patikimumo užtikrinimo paslaugos būtų akivaizdžiai atskirtos nuo kitų patikimumo užtikrinimo paslaugų, taip prisidedant prie rinkos skaidrumo. Kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai ES pasitikėjimo ženklą turėtų naudoti savanoriškai ir dėl tokio naudojimo neturėtų atsirasti kitų, nei šiame reglamente numatytų, reikalavimų;
- (48) nors siekiant užtikrinti abipusį elektroninių parašų pripažinimą būtinas aukštas saugumo lygis, tam tikrais atvejais, kaip antai susijusiais su Komisijos sprendimu 2009/767/EB <sup>(1)</sup>, taip pat turėtų būti priimami elektroniniai parašai, kuriais užtikrinamas žemesnio lygio saugumas;
- (49) šiuo reglamentu turėtų būti nustatytas principas, kad negalima atsisakyti pripažinti elektroninio parašo teisinės galios tik dėl to, kad parašas yra elektroninis arba kad jis neatitinka kvalifikuoto elektroninio parašo reikalavimų. Tačiau elektroninių parašų teisinė galia turi būti reglamentuojama nacionalinės teisės aktuose, išskyrus šiame reglamente numatytus reikalavimus, pagal kuriuos kvalifikuoto elektroninio parašo teisinė galia turėtų būti lygiavertė rašytiniam parašui;
- (50) kadangi valstybių narių kompetentingos institucijos dabar naudoja įvairaus formato pažangiuosius elektroninius parašus savo dokumentams pasirašyti elektroniniu būdu, būtina užtikrinti, kad valstybės narės, priimdamos elektroniniu būdu pasirašytus dokumentus, gebėtų techniškai apdoroti bent keletą pažangiojo elektroninio parašo formatų. Atitinkamai, kai valstybių narių kompetentingos institucijos naudoja pažangiuosius elektroninius spaudus, reikėtų užtikrinti, kad jos gebėtų patvirtinti bent kelių formatų pažangiuosius elektroninius spaudus;
- (51) pasirašančiam asmeniui turėtų būti sudaryta galimybė kvalifikuotų elektroninio parašo kūrimo įtaisų priežiūrą pavesti trečiajam šaliai su sąlyga, kad įdiegti tinkami mechanizmai ir procedūros, skirti užtikrinti, jog elektroninio parašo kūrimo duomenų naudojimą kontroliuoja tik pasirašantis asmuo ir kad naudojant įtaisą laikomasi kvalifikuotam elektroniniam parašui keliamų reikalavimų;
- (52) nuotolinių elektroninių parašų kūrimas, kai šio elektroninio parašo kūrimo aplinką valdo patikimumo užtikrinimo paslaugos teikėjas pasirašančio asmens vardu, turėtų plėstis dėl įvairiapusės jo ekonominės naudos. Vis dėlto siekiant užtikrinti, kad tokie elektroniniai parašai būtų teisiškai pripažįstami taip pat kaip ir vien vartotojo valdomoje aplinkoje sukurti elektroniniai parašai, nuotolinio elektroninio parašo paslaugos teikėjai turėtų taikyti konkrečias valdymo bei administracines saugumo procedūras ir naudoti patikimas sistemas bei produktus, įskaitant saugius elektroninius ryšių kanalus, siekiant užtikrinti, kad elektroninio parašo kūrimo aplinka būtų patikima ir kad ji būtų naudojama prižiūrint vien pasirašančiam asmeniui. Kai kvalifikuotas elektroninis parašas sukurtas naudojant nuotolinio elektroninio parašo kūrimo įtaisą, turėtų būti taikomi šiame reglamente nustatyti kvalifikuotiems patikimumo užtikrinimo paslaugos teikėjams keliami reikalavimai;

<sup>(1)</sup> 2009 m. spalio 16 d. Komisijos sprendimas 2009/767/EB, kuriuo pagal Europos Parlamento ir Tarybos direktyvą 2006/123/EB dėl paslaugų vidaus rinkoje nustatomos priemonės procedūroms, atliekamoms naudojantis elektroninėmis priemonėmis ir kontaktinių centrų paslaugomis, palengvinti (OL L 274, 2009 10 20, p. 36).

- (53) kvalifikuotų sertifikatų galiojimo sustabdymas yra įprasta patikimumo paslaugų teikėjų darbo praktika keliose valstybėse narėse; tai nėra atšaukimas ir dėl to sertifikatas laikinai netenka galios. Siekiant užtikrinti teisinį tikrumą, visada turi būti aiškiai nurodytas sertifikato statusas – galiojimas sustabdytas. Tuo tikslu patikimumo užtikrinimo paslaugų teikėjai turėtų būti atsakingi už tai, kad būtų aiškiai nurodytas sertifikato statusas, o galiojimo sustabdymo atveju – konkretus laikotarpis, kuriuo sertifikato galiojimas sustabdytas. Šiuo reglamentu neturėtų būti nustatoma, kad patikimumo užtikrinimo paslaugų teikėjai ar valstybės narės privalo taikyti sustabdymą, tačiau turėtų būti nustatytos skaidrumo taisyklės, kada ir kokiais atvejais galima taikyti tokią praktiką;
- (54) tarpvalstybinis sąveikumas ir kvalifikuotų sertifikatų pripažinimas yra tarpvalstybinio kvalifikuotų elektroninių parašų pripažinimo prielaida. Todėl kvalifikuotiems sertifikatams neturėtų būti taikoma jokių privalomų reikalavimų, viršijančių šiame reglamente nustatytus reikalavimus. Vis dėlto nacionaliniu lygiu kvalifikuotuose sertifikatuose turėtų būti leidžiama naudoti specifinius požymius, kaip antai unikalius atpažinimo ženklus, su sąlyga, kad tokie specifiniai požymiai netrukdo tarpvalstybiniam sąveikumui ir kvalifikuotų sertifikatų bei elektroninių parašų pripažinimui;
- (55) IT saugumo sertifikavimas, grindžiamas tarptautiniais standartais tokiais kaip antai ISO 15408 bei atitinkamais vertinimo metodais ir abipusio pripažinimo susitarimais, yra svarbi priemonė siekiant patikrinti kvalifikuotų elektroninio parašo kūrimo įtaisų saugumą ir jis turėtų būti skatinamas. Vis dėlto novatoriški sprendimai ir paslaugos, kaip antai mobilusis elektroninis parašas ir debesijos elektroninis parašas, yra paremti kvalifikuotų elektroninio parašo kūrimo įtaisų, kurių saugumo standartų dar gali ir nebūti arba dar tik vyksta pirmasis IT saugumo sertifikavimas, techniniu ir organizaciniu sprendimu. Tokių kvalifikuotų elektroninio parašo kūrimo įtaisų saugumo lygis galėtų būti įvertintas taikant alternatyvius procesus tik tuo atveju, kai tokių saugumo standartų dar nėra ir kai vyksta pirmasis IT saugumo sertifikavimas. Tie procesai turėtų būti panašūs į IT saugumo sertifikavimo standartus tiek, kad jų saugumo lygiai būtų lygiaverčiai. Tuos procesus galėtų palengvinti tarpusavio vertinimas;
- (56) šiame reglamente turėtų būti nustatyti kvalifikuotiems elektroninio parašo kūrimo įtaisams keliami reikalavimai, siekiant užtikrinti pažangiųjų elektroninių parašų funkcionalumą. Šis reglamentas neturėtų būti taikomas visai sistemos aplinkai, kurioje veikia tokia įranga. Todėl kvalifikuotų parašo kūrimo įtaisų sertifikavimas turėtų būti taikomas tik aparatinei ir sistemos programinei įrangai, naudojamai parašo kūrimo įtaisų sukurtiems, saugomiems arba apdorotiems parašo kūrimo duomenims valdyti ir juos apsaugoti. Kaip išsamiai nurodyta atitinkamuose standartuose, sertifikavimo pareiga neturėtų būti taikoma parašo kūrimo taikomosioms programoms;
- (57) siekiant užtikrinti parašo galiojimo teisinį tikrumą, labai svarbu išsamiai nurodyti, kokias kvalifikuoto elektroninio parašo sudedamąsias dalis turėtų įvertinti galiojimą tvirtinanti pasikliaujančioji šalis. Be to, reikalavimų nustatymas kvalifikuotiems patikimumo užtikrinimo paslaugų teikėjams, kurie gali teikti kvalifikuotą galiojimo patvirtinimo paslaugą pasikliaujančiosioms šalims, kurios pačios nenori arba negali atlikti kvalifikuotų elektroninių parašų galiojimo patvirtinimo, turėtų paskatinti privatųjį ir viešąjį sektorių investuoti į tokias paslaugas. Įgyvendinus abu šiuos elementus, kvalifikuoto elektroninio parašo galiojimo patvirtinimas Sąjungos lygmeniu turėtų tapti lengvas ir patogus visoms šalims;
- (58) kai operacijai atlikti reikalingas juridinio asmens kvalifikuotas elektroninis spaudas, lygiai taip pat turėtų būti priimamas to juridinio asmens įgaliotojo atstovo kvalifikuotas elektroninis parašas;
- (59) elektroniniai spaudai turėtų būti įrodymas, kad elektroninį dokumentą išdavė juridinis asmuo, užtikrinant dokumento kilmę ir vientisumą;
- (60) kvalifikuotus elektroninių spaudų sertifikatus išduodantys patikimumo užtikrinimo paslaugų teikėjai turėtų įgyvendinti priemones, būtinas nustatyti fizinio asmens, atstovaujančio juridiniam asmeniui, kuriam suteiktas kvalifikuotas elektroninio spaudo sertifikatas, tapatybę, kai toks tapatybės nustatymas būtinas nacionaliniu lygiu, atsižvelgiant į teismo ar administracinius procesus;



- (61) šiuo reglamentu turėtų būti užtikrinta ilgalaikis informacijos išsaugojimas, t. y. siekiant užtikrinti elektroninio parašo ir elektroninių spaudų teisinį galiojimą ilgą laiką ir garantuoti, kad jų galiojimas būtų patvirtintas nepaisant būsimų technologinių pokyčių;
- (62) siekiant užtikrinti kvalifikuotų elektroninių laiko žymų saugumą, šiuo reglamentu turėtų būti reikalaujama naudoti pažangųjį elektroninį spaudą arba pažangųjį elektroninį parašą arba kitus lygiaverčius metodus. Numatoma, kad dėl inovacijų gali atsirasti naujos technologijos, kuriomis būtų galima užtikrinti lygiavertį laiko žymų saugumo lygį. Kai naudojamas kitas, ne pažangiojo elektroninio spaudo ar pažangiojo elektroninio parašo, metodas, kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai atitikties turėtų įvertinimo ataskaitose įrodyti, kad tokiu metodu užtikrinamas lygiavertis saugumo lygis ir laikomasi šiame reglamente nustatytų pareigų;
- (63) elektroniniai dokumentai yra svarbūs tolesnei tarpvalstybinių elektroninių operacijų vidaus rinkoje plėtrai. Šiame reglamente turėtų būti nustatomas principas, kad negalima atsisakyti pripažinti elektroninio dokumento teisinės galios tik dėl to, kad dokumentas yra elektroninis siekiant užtikrinti, kad elektroninė operacija nebūtų atmesta tik dėl to, kad dokumentas yra elektroninis;
- (64) spręsdama pažangiųjų elektroninių parašų ir spaudų formatų klausimus, Komisija turėtų remtis šiuo metu taikoma praktika, standartais ir teisės aktais, ypač Komisijos sprendimu 2011/130/ES <sup>(1)</sup>;
- (65) be juridinio asmens išduoto dokumento tapatumo nustatymo, elektroniniai spaudai gali būti naudojami siekiant nustatyti bet kokio juridinio asmens skaitmeninio turto, kaip antai programinės įrangos kodo ar serverių, tapatumą;
- (66) 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;
- (67) naudodamasis interneto svetainių tapatumo nustatymo paslaugomis interneto svetainės lankytojas gali būti tikras, kad interneto svetainė priklauso tikram ir teisėtam subjektui. Tos paslaugos prisideda prie pasitikėjimo kūrimo ir suteikia drąsos vykdyti verslą internetu, nes vartotojai pasitikės interneto svetaine, kurios tapatumas nustatytas. Interneto svetainės tapatumo nustatymo paslaugų teikimas ir naudojimas yra visiškai savanoriškas. Vis dėlto norint, kad interneto svetainės tapatumo nustatymas taptų pasitikėjimo didinimo priemone, kuri pagerintų vartotojo patirtį ir toliau skatintų vidaus rinkos augimą, šiame reglamente teikėjams ir jų paslaugoms turėtų būti nustatytos minimalios saugumo ir atsakomybės pareigos. Tuo tikslu buvo atsižvelgta į šiuo metu sektoriuje įgyvendinamų iniciatyvų, pavyzdžiui, Sertifikavimo institucijų ir naršyklių verslo forumo – CA/B Forumas rezultatus. Be to, šiuo reglamentu neturėtų būti trukdoma naudoti kitų interneto svetainės tapatumo nustatymo priemonių ar metodų, kuriems netaikomas šis reglamentas, ir kliudoma trečiųjų valstybių interneto svetainės tapatumo nustatymo paslaugų teikėjams teikti savo paslaugas Sąjungoje esantiems klientams. Vis dėlto trečiosios valstybės teikėjo interneto svetainės tapatumo nustatymo paslaugos turėtų būti pripažintos kvalifikuotomis pagal šį reglamentą, tik jeigu Sąjunga ir valstybė, kurioje įsisteigęs teikėjas, yra sudariusios tarptautinį susitarimą;
- (68) remiantis Sutarties dėl Europos Sąjungos veikimo (toliau – SESV) nuostatomis dėl įsisteigimo pagal juridinių asmenų sąvoką veiklos vykdytojai gali laisvai pasirinkti teisinę formą, kuri, jų manymu, yra tinkama jų veiklai vykdyti. Todėl juridiniai asmenys, kaip apibrėžta SESV, yra visi subjektai, kurie yra įsteigti pagal valstybės narės teisės aktus arba kurie yra reglamentuojami tokiais teisės aktais, neatsižvelgiant į jų teisinę formą;
- (69) Sąjungos institucijos, įstaigos ir agentūros administracinio bendradarbiavimo tikslu yra skatinamos pripažinti elektroninę atpažintį ir patikimumo užtikrinimo paslaugas, kurioms taikomas šis reglamentas, remiantis visų pirma esama gerąja praktika ir šiuo metu vykdomų projektų rezultatais srityse, kurioms taikomas šis reglamentas;

<sup>(1)</sup> 2011 m. vasario 25 d. Komisijos sprendimas 2011/130/ES, kuriuo nustatomi būtinieji dokumentų, kompetentingų institucijų pasirašomų elektroniniu būdu pagal Europos Parlamento ir Tarybos direktyvą 2006/123/EB dėl paslaugų vidaus rinkoje, tarptautinio tvarkymo reikalavimai (OL L 53, 2011 2 26, p. 66).

- (70) siekiant lanksčiai ir greitai papildyti tam tikrus šio reglamento išsamius techninius aspektus, pagal SESV 290 straipsnį Komisijai turėtų būti deleguoti įgaliojimai priimti aktus dėl kriterijų, kuriuos turi atitikti už kvalifikuotų elektroninio parašo kūrimo įtaisų sertifikavimą atsakingos įstaigos. Ypač svarbu, kad atlikdama parengiamąjį darbą Komisija tinkamai konsultuotųsi, taip pat ir su ekspertais. Atlikdama su deleguotaisiais aktais susijusį parengiamąjį darbą ir rengdama jų tekstus Komisija turėtų užtikrinti, kad atitinkami dokumentai būtų vienu metu, laiku ir tinkamai perduodami Europos Parlamentui ir Tarybai;
- (71) siekiant užtikrinti vienodas šio reglamento įgyvendinimo sąlygas, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai, visų pirma tam, kad ji nurodytų standartų, kurių laikantis būtų suteikiama prezumpcija dėl atitikties tam tikriems šiame reglamente nustatytiems reikalavimams užtikrinimo, referencinius numerius. Tais įgaliojimais turėtų būti naudojamosi laikantis Europos Parlamento ir Tarybos reglamento (ES) Nr. 182/2011 <sup>(1)</sup>;
- (72) priimdama deleguotuosius arba įgyvendinimo aktus Komisija turėtų deramai atsižvelgti į Europos ir tarptautinių standartizacijos organizacijų ir įstaigų, visų pirma Europos standartizacijos komiteto (CEN), Europos telekomunikacijų standartų instituto (ETSI), Tarptautinės standartizacijos organizacijos (ISO) ir Tarptautinės telekomunikacijų sąjungos (ITU) parengtus standartus bei technines specifikacijas, kad būtų užtikrintas aukštas elektroninės atpažinties ir patikimumo užtikrinimo paslaugų saugumo lygis;
- (73) dėl teisinio tikrumo ir aiškumo Direktyva 1999/93/EB turėtų būti panaikinta;
- (74) siekiant užtikrinti teisinį tikrumą rinkos dalyviams, kurie jau naudoja pagal Direktyvą 1999/93/EB fiziniams asmenims išduotus kvalifikuotus sertifikatus, reikia numatyti pakankamą pereinamąjį laikotarpį. Lygiai taip pat reikėtų nustatyti pereinamojo laikotarpio priemones dėl pažangaus parašo kūrimo įtaisų, kurių atitiktis buvo nustatyta pagal Direktyvą 1999/93/EB, ir pereinamojo laikotarpio priemones sertifikavimo paslaugų teikėjams, kurie išduos sertifikatus anksčiau nei 2016 m. liepos 1 d. Galiausiai, taip pat reikia suteikti Komisijai galimybę iki tos datos priimti įgyvendinimo ir deleguotuosius aktus;
- (75) šiame reglamente nustatyti taikymo terminai nedaro poveikio jau turimiems valstybių narių išpareigojimams pagal Sąjungos teisę, visų pirma pagal Direktyvą 2006/123/EB;
- (76) kadangi šio reglamento tikslų, valstybės narės negali deramai pasiekti, o dėl siūlomo veiksmo masto ir poveikio tų tikslų būtų geriau siekti Sąjungos lygiu, laikydamosi Europos Sąjungos sutarties 5 straipsnyje nustatyto subsidarumo principo Sąjunga gali priimti priemones. Pagal tame straipsnyje nustatytą proporcingumo principą šiuo reglamentu neviršijama to, kas būtina tiems tikslams pasiekti;
- (77) vadovaujantis Europos Parlamento ir Tarybos reglamento (EB) Nr. 45/2001 <sup>(2)</sup> 28 straipsnio 2 dalimi buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu, kuris pateikė nuomonę 2012 m. rugsėjo 27 d. <sup>(3)</sup>,

<sup>(1)</sup> 2011 m. vasario 16 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 182/2011, kuriuo nustatomos valstybių narių vykdomos Komisijos naudojimosi įgyvendinimo įgaliojimais kontrolės mechanizmų taisyklės ir bendrieji principai (OL L 55, 2011 2 28, p. 13).

<sup>(2)</sup> 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (OL L 8, 2001 1 12, p. 1).

<sup>(3)</sup> OL C 28, 2013 1 30, p. 6.

PRIĖMĖ ŠĮ REGLAMENTĄ:

## I SKYRIUS

### BENDROSIOS NUOSTATOS

#### 1 straipsnis

##### Dalykas

Siekiant užtikrinti tinkamą vidaus rinkos veikimą, kartu siekiant tinkamo elektroninės atpažinties priemonių ir patikimumo užtikrinimo paslaugų saugumo lygio, šiuo reglamentu:

- a) nustatomos sąlygos, kuriomis valstybės narės pripažįsta fizinių ir juridinių asmenų elektroninės atpažinties priemones, kurioms taikoma kitos valstybės narės elektroninės atpažinties schema, apie kurią pranešta;
- b) nustatomos patikimumo užtikrinimo paslaugų, visų pirma elektroninių operacijų, taisyklės, ir
- c) nustatoma elektroninių parašų, elektroninių spaudų, elektroninių laiko žymų, elektroninių dokumentų, elektroninio registruoto pristatymo paslaugų ir interneto svetainių tapatumo nustatymo sertifikavimo paslaugų teisinė sistema.

#### 2 straipsnis

##### Taikymo sritis

1. Šis reglamentas taikomas elektroninės atpažinties schemoms, apie kurias pranešė valstybė narė, ir Sąjungoje įsistėjusiems patikimumo užtikrinimo paslaugų teikėjams.
2. Šis reglamentas netaikomas patikimumo užtikrinimo paslaugų, kuriomis naudojamos tik uždaroje sistemoje, sukurtose pagal nacionalinės teisės aktus arba apibrėžtose dalyvių grupės susitarimais, teikimui.
3. Šis reglamentas nedaro poveikio nacionalinės arba Sąjungos teisės aktams, susijusiems su sutarčių sudarymu arba kitų teisinių ar procedūrinių pareigų nustatymu ir šių sutarčių bei pareigų galiojimu, susijusių su forma.

#### 3 straipsnis

##### Terminų apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

1. elektroninė atpažintis – elektroninių asmens tapatybės duomenų, kuriais nurodomas konkretus fizinis ar juridinis asmuo arba juridiniam asmeniui atstovaujantis fizinis asmuo, naudojimo procesas;
2. elektroninės atpažinties priemonė – materialus ir (arba) nematerialus objektas su asmens tapatybės duomenimis, naudojamas internetinės paslaugos tapatumui nustatyti;
3. asmens tapatybės duomenys – duomenų rinkinys, pagal kurį galima nustatyti fizinio ar juridinio asmens arba juridiniam asmeniui atstovaujantį fizinio asmens tapatybę;
4. elektroninės atpažinties schema – elektroninės atpažinties sistema, pagal kurią fiziniams ar juridiniams asmenims arba juridiniams asmenims atstovaujantiems fiziniams asmenims išduodamos elektroninės atpažinties priemonės;

5. tapatumo nustatymas – elektroninis procesas, leidžiantis patvirtinti fizinio arba juridinio asmens elektroninę atpažintį arba elektroninės formos duomenų kilmę ir vientisumą;
6. pasikliaujančioji šalis – fizinis arba juridinis asmuo, kuris pasikliauja elektronine atpažintimi ar patikimumo užtikrinimo paslauga;
7. viešojo sektoriaus įstaiga – valstybės, regioninė arba vietos valdžios institucija, viešosios teisės reglamentuojama įstaiga ar vienos arba kelių tokių institucijų arba vienos ar kelių tokių viešosios teisės reglamentuojamų įstaigų sudaryta asociacija arba bent vienos iš šių institucijų, įstaigų ar asociacijų teikti viešąsias paslaugas įgaliotas privatusis subjektas, kai jis veikia pagal toki įgaliojimą;
8. viešosios teisės reglamentuojamas subjektas – subjektas, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2014/24/ES <sup>(1)</sup> 2 straipsnio 1 dalies 4 punkte;
9. pasirašantis asmuo – fizinis asmuo, kuris sukuria elektroninį parašą;
10. elektroninis parašas – elektroninės formos duomenys, kurie yra prijungti prie kitų elektroninės formos duomenų arba logiškai susieti su jais ir kuriuos pasirašantis asmuo naudoja pasirašydamas;
11. pažangusis elektroninis parašas – elektroninis parašas, atitinkantis 26 straipsnyje nustatytus reikalavimus;
12. kvalifikuotas elektroninis parašas – pažangusis elektroninis parašas, sukurtas naudojant kvalifikuotą elektroninio parašo kūrimo įtaisą ir patvirtintas kvalifikuotu elektroninio parašo sertifikatu;
13. elektroninio parašo kūrimo duomenys – unikalūs duomenys, kuriuos pasirašantis asmuo naudoja kurdamas elektroninį parašą;
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;
15. kvalifikuotas elektroninio parašo sertifikatas – elektroninio parašo sertifikatas, kurį išduoda kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas ir kuris atitinka I priede nustatytus reikalavimus;
16. patikimumo užtikrinimo paslauga – elektroninė paslauga, kuri paprastai teikiama už atlygį ir kurią sudaro:
  - a) elektroninių parašų, elektroninių spaudų arba elektroninių laiko žymų kūrimas, patikrinimas ir patvirtinimas, elektroninio registruoto pristatymo paslaugos ir su tomis paslaugomis susiję sertifikatai arba
  - b) interneto svetainių tapatumo nustatymo sertifikatų kūrimas, patikrinimas ir patvirtinimas, arba
  - c) elektroninių parašų, spaudų arba su tomis paslaugomis susijusių sertifikatų ilgalaikis išsaugojimas;
17. kvalifikuota patikimumo užtikrinimo paslauga – šiame reglamente nustatytus taikytinus reikalavimus atitinkanti patikimumo užtikrinimo paslauga;

<sup>(1)</sup> 2014 m. vasario 26 d. Europos Parlamento ir Tarybos direktyva 2014/24/ES dėl viešųjų pirkimų, kuria panaikinama Direktyva 2004/18/EB (OL L 94, 2014 3 28, p. 65).

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;
19. patikimumo užtikrinimo paslaugų teikėjas – fizinis arba juridinis asmuo, teikiantis vieną arba daugiau patikimumo užtikrinimo paslaugų arba kaip kvalifikuotas, arba kaip nekvalifikuotas patikimumo užtikrinimo paslaugų teikėjas;
20. kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas – patikimumo užtikrinimo paslaugų teikėjas, teikiantis vieną ar daugiau kvalifikuotų patikimumo užtikrinimo paslaugų, kuriam priežiūros įstaiga yra suteikusi kvalifikacijos statusą;
21. produktas – aparatinė arba programinė įranga, arba svarbios aparatinės arba programinės įrangos sudedamosios dalys, skirtos naudoti teikiant patikimumo užtikrinimo paslaugas;
22. elektroninio parašo kūrimo įtaisas – sukonfigūruota programinė arba aparatinė įranga, naudojama elektroniniam parašui kurti;
23. kvalifikuotas elektroninio parašo kūrimo įtaisas – elektroninio parašo kūrimo įtaisas, atitinkantis II priede nustatytus reikalavimus;
24. spaudo kūrėjas – juridinis asmuo, kuris sukuria elektroninį spaudą;
25. elektroninis spaudas – elektroninės formos duomenys, prijungti prie kitų elektroninės formos duomenų arba su jais logiškai susieti, kad būtų užtikrinta pastarųjų kilmė ir vientisumas;
26. pažangusis elektroninis spaudas – elektroninis spaudas, atitinkantis 36 straipsnyje nustatytus reikalavimus;
27. kvalifikuotas elektroninis spaudas – pažangusis elektroninis spaudas, sukurtas naudojant kvalifikuotą elektroninio spaudo kūrimo įtaisą ir patvirtintas kvalifikuotu elektroninio spaudo sertifikatu;
28. elektroninio spaudo kūrimo duomenys – unikalūs duomenys, kuriuos elektroninio spaudo kūrėjas naudoja kurdamas elektroninį spaudą;
29. elektroninio spaudo sertifikatas – elektroninis liudijimas, kuriuo elektroninio spaudo patvirtinimo duomenys susiejami su juridiniu asmeniu ir kuriuo patvirtinamas to asmens pavadinimas;
30. kvalifikuotas elektroninio spaudo sertifikatas – elektroninio spaudo sertifikatas, kurį išduoda kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas ir kuris atitinka III priede nustatytus reikalavimus;
31. elektroninio spaudo kūrimo įtaisas – sukonfigūruota programinė arba aparatinė įranga, naudojama elektroniniam spaudui kurti;
32. kvalifikuotas elektroninio spaudo kūrimo įtaisas – elektroninio spaudo kūrimo įtaisas, atitinkantis *mutatis mutandis* II priede nustatytus reikalavimus;
33. elektroninė laiko žyma – elektroninės formos duomenys, kuriais kiti elektroninės formos duomenys susiejami su tam tikru laiku ir taip sukuriamas įrodymas, kad pastarieji egzistavo tuo metu;
34. kvalifikuota elektroninė laiko žyma – elektroninė laiko žyma, atitinkanti 42 straipsnyje nustatytus reikalavimus;



35. elektroninis dokumentas – bet koks turinys, saugomas elektronine forma, visų pirma tekstas ar garsas, vaizdo arba garso ir vaizdo įrašas;
36. elektroninio registruoto pristatymo paslauga – paslauga, kuria sudaroma galimybė perduoti duomenis elektroninėmis priemonėmis tarp trečiųjų šalių ir kuria suteikiama su perduodamų duomenų tvarkymu susijusių įrodymų, įskaitant duomenų išsiuntimo ir gavimo įrodymą, ir kuria perduodami duomenys apsaugomi nuo praradimo, vagystės, sugadinimo arba neteisėto pakeitimo rizikos;
37. kvalifikuota elektroninio registruoto pristatymo paslauga – elektroninio registruoto pristatymo paslauga, atitinkanti 44 straipsnyje nustatytus reikalavimus;
38. interneto svetainės tapatumo nustatymo sertifikatas – liudijimas, suteikiantis galimybę nustatyti interneto svetainės tapatumą ir susiejantis interneto svetainę su fiziniu ar juridiniu asmeniu, kuriam buvo išduotas sertifikatas;
39. kvalifikuotas interneto svetainės tapatumo nustatymo sertifikatas – interneto svetainės tapatumo nustatymo sertifikatas, kurį išduoda kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas ir kuris atitinka IV priede nustatytus reikalavimus;
40. patvirtinimo duomenys – duomenys, naudojami patvirtinti elektroninio parašo arba elektroninio spaudo galiojimą;
41. patvirtinimas – patikrinimo ir patvirtinimo, kad elektroninis parašas ar spaudas galioja, procedūra.

#### 4 straipsnis

##### **Vidaus rinkos principas**

1. Dėl priežasčių, kurios patenka į šio reglamento reglamentuojamas sritis, valstybės narės teritorijoje patikimumo užtikrinimo paslaugas patikimumo užtikrinimo paslaugų teikėjas, įsisteigęs kitoje valstybėje narėje, gali teikti be apribojimų.
2. Šį reglamentą atitinkančius produktus ir patikimumo užtikrinimo paslaugas leidžiama laisvai platinti vidaus rinkoje.

#### 5 straipsnis

##### **Duomenų tvarkymas ir apsauga**

1. Asmens duomenys tvarkomi laikantis Direktyvos 95/46/EB.
2. Nedarant poveikio slapyvardžiams suteiktai teisei galiai pagal nacionalinę teisę, vykdant elektronines operacijas nedraudžiama naudoti slapyvardžių.

## II SKYRIUS

### **ELEKTRONINĖ ATPAŽINTIS**

#### 6 straipsnis

##### **Abipusis pripažinimas**

1. Kai pagal nacionalinės teisės aktus arba nacionalinę administracinę praktiką reikalaujama, kad norint vienoje valstybėje narėje pasinaudoti viešojo sektoriaus įstaigos teikiama internetine paslauga būtina užtikrinti elektroninę atpažintį naudojant elektronines atpažinties priemones ir tapatumo nustatymą, tos internetinės paslaugos tarpvalstybinio tapatumo nustatymo tikslais pirmojoje valstybėje narėje pripažįstamos kitoje valstybėje narėje išduotos elektroninės atpažinties priemonės, su sąlyga, kad įvykdomos šios sąlygos:

- a) elektroninės atpažinties priemonė yra išduota pagal elektroninės atpažinties schemą, kuri yra įtraukta į Komisijos pagal 9 straipsnį skelbiamą sąrašą;

- b) elektroninės atpažinties priemonės saugumo užtikrinimo lygis atitinka saugumo užtikrinimo lygį, kuris yra lygiavertis saugumo užtikrinimo lygiui, kurio reikalauja atitinkama viešojo sektoriaus įstaiga, kad būtų galima pasinaudoti ta internetine paslauga pirmojoje valstybėje narėje, arba yra už jį aukštesnis, su sąlyga, kad tos elektroninės atpažinties priemonės saugumo užtikrinimo lygis atitinka pakankamą arba aukštą saugumo užtikrinimo lygį;
- c) atitinkama viešojo sektoriaus įstaiga taiko pakankamą arba aukštą saugumo užtikrinimo lygį galimybės naudotis ta internetine paslauga atžvilgiu.

Toks pripažinimas atliekamas ne vėliau kaip per 12 mėnesių po to, kai Komisija paskelbia sąrašą, nurodytą pirmos pastraipos a punkte.

2. Elektroninės atpažinties priemonė, išduota pagal į Komisijos pagal 9 straipsnį paskelbtą sąrašą įtrauktą elektroninės atpažinties schemą ir atitinkanti žemą saugumo užtikrinimo lygį, gali būti viešojo sektoriaus įstaigų pripažįstama tų įstaigų teikiamos internetinės paslaugos tarpvalstybinio tapatumo nustatymo tikslais.

#### 7 straipsnis

##### **Pranešimo apie elektroninės atpažinties schemas atitiktis reikalavimams**

Elektroninės atpažinties schema atitinka pranešimo apie ją pagal 9 straipsnio 1 dalį reikalavimus, su sąlyga, kad įvykdomos visos šios sąlygos:

- a) elektroninės atpažinties priemonės pagal elektroninės atpažinties schemą yra išduotos:
  - i) pranešančiosios valstybės narės;
  - ii) pagal pranešančiosios valstybės narės suteiktą įgaliojimą ar
  - iii) nepriklausomai nuo pranešančiosios valstybės narės ir yra tos valstybės narės pripažintos;
- b) elektroninės atpažinties priemonės pagal elektroninės atpažinties schemą gali būti naudojamos norint pasinaudoti bent viena viešojo sektoriaus įstaigos teikiama paslauga, kuria reikalaujama užtikrinti elektroninę atpažintį pranešančiojoje valstybėje narėje;
- c) elektroninės atpažinties schema ir pagal ją išduodamos elektroninės atpažinties priemonės tenkina bent vieno iš saugumo užtikrinimo lygių reikalavimus, nustatytus 8 straipsnio 3 dalyje nurodytame įgyvendinimo akte;
- d) pranešančioji valstybė narė užtikrina, kad asmens tapatybės duomenys, kuriais nurodomas konkretus atitinkamas asmuo, būtų susieti su 3 straipsnio 1 punkte nurodytu fiziniu arba juridiniu asmeniu elektroninės atpažinties priemonės išdavimo pagal tą schemą metu, laikantis atitinkamo saugumo užtikrinimo lygio techninių specifikacijų, standartų ir procedūrų, nustatytų 8 straipsnio 3 dalyje nurodytame įgyvendinimo akte;
- e) elektroninę atpažinties priemonę pagal tą schemą išduodanti šalis užtikrina, kad elektroninė atpažinties priemonė būtų susieta su šio straipsnio d punkte nurodytu asmeniu, laikantis atitinkamo saugumo užtikrinimo lygio techninių specifikacijų, standartų ir procedūrų, nustatytų 8 straipsnio 3 dalyje nurodytame įgyvendinimo akte;
- f) pranešančioji valstybė narė užtikrina tapatumo nustatymo internete galimybę, kad bet kuri pasikliaujančioji šalis, įsteigta kitos valstybės narės teritorijoje, galėtų patvirtinti gautus elektroninės formos asmens tapatybės duomenis.

Pasikliaujančiosioms šalims, kurios nėra viešojo sektoriaus įstaigos, pranešančioji valstybė narė gali nustatyti naudoti ta tapatumo nustatymo galimybe tvarką. Tarpvalstybinis tapatumo nustatymas yra nemokamas, kai jis susijęs su viešojo sektoriaus įstaigos teikiama internetine paslauga.

Valstybės narės nenustato pasikliaujančiosioms šalims, kurios ketina atlikti tokių tapatumo nustatymą, jokių specialių neproporcingų techninių reikalavimų, kai dėl tokių reikalavimų užkertamas kelias arba kyla esminių kliūčių elektroninės atpažinties schemų, apie kurias pranešta, sąveikumui;

- g) bent prieš šešis mėnesius iki pranešimo pagal 9 straipsnio 1 dalį pranešančioji valstybė narė kitoms valstybėms narėms 12 straipsnio 5 dalyje nustatytos pareigos įvykdymo tikslais pateikia tos schemos aprašymą pagal procedūrinės sąlygas, nustatytas 12 straipsnio 7 dalyje nurodytuose įgyvendinimo aktuose;
- h) elektroninės atpažinties schema atitinka 12 straipsnio 8 dalyje nurodytame įgyvendinimo akte nustatytus reikalavimus.

#### 8 straipsnis

### Elektroninės atpažinties schemų saugumo užtikrinimo lygiai

1. Elektroninės atpažinties schemoje, apie kurią pranešta pagal 9 straipsnio 1 dalį, apibrėžiami elektroninės atpažinties priemonių, išduodamų pagal tą schemą, žemas, pakankamas ir (arba) aukštas saugumo užtikrinimo lygiai.
2. Žemas, pakankamas ir aukštas saugumo užtikrinimo lygiai atitinkamai atitinka šiuos kriterijus:
  - a) žemas saugumo užtikrinimo lygis grindžiamas elektroninės atpažinties priemone elektroninės atpažinties schemos kontekste, kuria užtikrinamas ribotas pareikštos arba patvirtintos asmens tapatybės patikimumo laipsnis ir kuri apibūdinama remiantis su ja susijusiomis techninėmis specifikacijomis, standartais ir procedūromis, įskaitant technines kontrolės priemones, kurių paskirtis – sumažinti netinkamo pasinaudojimo tapatybe arba jos pakeitimo riziką;
  - b) pakankamas saugumo užtikrinimo lygis grindžiamas elektroninės atpažinties priemone elektroninės atpažinties schemos kontekste, kuria užtikrinamas pakankamas pareikštos arba patvirtintos asmens tapatybės patikimumo laipsnis ir kuri apibūdinama remiantis su ja susijusiomis techninėmis specifikacijomis, standartais ir procedūromis, įskaitant technines kontrolės priemones, kurių paskirtis – labai sumažinti netinkamo pasinaudojimo tapatybe arba jos pakeitimo riziką;
  - c) aukštas saugumo užtikrinimo lygis grindžiamas elektroninės atpažinties priemone elektroninės atpažinties schemos kontekste, kuria užtikrinamas aukštesnis pareikštos arba patvirtintos asmens tapatybės patikimumo laipsnis nei pakankamo saugumo užtikrinimo lygio elektroninės atpažinties priemone ir kuri apibūdinama remiantis su ja susijusiomis techninėmis specifikacijomis, standartais ir procedūromis, įskaitant technines kontrolės priemones, kurių paskirtis – užkirsti kelią netinkamam pasinaudojimui tapatybe arba jos pakeitimui.
3. Ne vėliau kaip 2015 m. rugsėjo 18 d., atsižvelgdama į atitinkamus tarptautinius standartus ir laikydama 2 dalies, Komisija priima įgyvendinimo aktus, kuriais nustato minimalias technines specifikacijas, standartus ir procedūras, kuriomis remiantis 1 dalies tikslais apibrėžiami elektroninės atpažinties priemonių žemas, pakankamas ir aukštas saugumo užtikrinimo lygiai.

Tos minimalios techninės specifikacijos, standartai ir procedūros nustatomi remiantis tuo, ar toliau nurodyti elementai yra patikimi ir kokybiški:

- a) fizinių ar juridinių asmenų, pateikusių prašymą išduoti elektroninės atpažinties priemones, tapatybės įrodymo ir patikrinimo procedūra;

- b) prašomų elektroninės atpažinties priemonių išdavimo procedūra;
- c) tapatumo nustatymo mechanizmas, kurį taikant fizinis arba juridinis asmuo naudojami elektroninės atpažinties priemonė, kad patvirtintų pasikliaujančiai šaliai savo tapatybę;
- d) elektroninės atpažinties priemonę išduodantis subjektas;
- e) bet kuri kita įstaiga, dalyvaujanti teikiant prašymą išduoti elektroninės atpažinties priemonę, ir
- f) išduotos elektroninės atpažinties priemonės techninės ir saugumo specifikacijos.

Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

#### 9 straipsnis

#### Pranešimas

1. Pranešančioji valstybė narė praneša Komisijai toliau nurodomą informaciją ir nedelsdama informuoja apie visus vėlesnius jos pakeitimus:

- a) elektroninės atpažinties schemos, apie kurią pranešama, aprašą, įskaitant jos saugumo užtikrinimo lygius ir elektroninės atpažinties priemonių pagal schemą išdavėją ar išdavėjus;
- b) taikytiną priežiūros režimą ir informaciją apie atsakomybės režimą, susijusius su:
  - i) elektroninės atpažinties priemonę išduodančia šalimi ir
  - ii) tapatumo nustatymo procedūrą vykdančia šalimi;
- c) valdžios instituciją arba institucijas, atsakingas už elektroninės atpažinties schemą;
- d) informaciją apie subjektą arba subjektus, kurie tvarko unikalių asmens tapatybės duomenų registraciją;
- e) aprašymą, kaip vykdomi 12 straipsnio 8 dalyje nurodytuose įgyvendinimo aktuose nustatyti reikalavimai;
- f) 7 straipsnio f punkte nurodyto tapatumo nustatymo aprašą;
- g) elektroninės atpažinties schemos, apie kurią pranešama, tapatumo nustatymo arba atitinkamų nepatikimų sudedamųjų dalių naudojimo sustabdymo arba atšaukimo nuostatas.

2. Praėjus vieneriems metams po 8 straipsnio 3 dalyje ir 12 straipsnio 8 dalyje nurodytų įgyvendinimo aktų taikymo pradžios dienos Komisija *Europos Sąjungos oficialiajame leidinyje* paskelbia elektroninės atpažinties schemų, apie kurias buvo pranešta pagal šio straipsnio 1 dalį, sąrašą ir pagrindinę informaciją apie šias schemas.

3. Jei Komisija gauna pranešimą pasibaigus 2 dalyje nurodytam laikotarpiui, ji per du mėnesius nuo to pranešimo gavimo dienos paskelbia *Europos Sąjungos oficialiajame leidinyje* 2 dalyje nurodyto sąrašo pakeitimus.

4. Valstybė narė gali pateikti Komisijai prašymą iš 2 dalyje nurodyto sąrašo išbraukti elektroninės atpažinties schemą, apie kurią pranešė ta valstybė narė. Komisija atitinkamus sąrašo pakeitimus *Europos Sąjungos oficialiajame leidinyje* paskelbia per vieną mėnesį nuo valstybės narės prašymo gavimo dienos.
5. Komisija gali priimti įgyvendinimo aktus, kuriais apibrėžia pranešimo teikimo pagal 1 dalį aplinkybes, formatus ir procedūras. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

#### 10 straipsnis

##### Apsaugos pažeidimas

1. Kai elektroninės atpažinties schema, apie kurią pranešta pagal 9 straipsnio 1 dalį, arba 7 straipsnio f punkte nurodytas tapatumo nustatymas pažeidžiami arba jų patikimumas iš dalies sumažėja taip, kad tai turi poveikio tos schemos tarpvalstybinio tapatumo nustatymo patikimumui, pranešančioji valstybė narė nedelsdama sustabdo arba atšaukia tą tarpvalstybinį tapatumo nustatymą arba atitinkamas nepatikimas sudedamąsias dalis ir apie tai informuoja kitas valstybes nares ir Komisiją.
2. Kai 1 dalyje nurodytas pažeidimas pašalinamas ar patikimumas atkuriamas, pranešančioji valstybė narė atkuria tarpvalstybinį tapatumo nustatymą ir nepagrįstai nedelsdama apie tai praneša kitoms valstybėms narėms ir Komisijai.
3. Jei per tris mėnesius nuo sustabdymo ar atšaukimo 1 dalyje nurodytas pažeidimas nepašalinamas ar patikimumas neatkuriamas, pranešančioji valstybė narė kitoms valstybėms narėms ir Komisijai praneša apie elektroninės atpažinties schemos panaikinimą.

Atitinkamus 9 straipsnio 2 dalyje nurodyto sąrašo pakeitimus Komisija nepagrįstai nedelsdama skelbia *Europos Sąjungos oficialiajame leidinyje*.

#### 11 straipsnis

##### Atsakomybė

1. Pranešančioji valstybė narė atsako už tyčia ar dėl neatsargumo bet kuriam fiziniam ar juridiniam asmeniui padarytą žalą dėl 7 straipsnio d ir f punktuose nustatytų pareigų nevykdymo atliekant tarpvalstybinę operaciją.
2. Elektroninės atpažinties priemonę išduodanti šalis atsako už tyčia ar dėl neatsargumo bet kuriam fiziniam ar juridiniam asmeniui padarytą žalą dėl 7 straipsnio e punkte nurodytos pareigos nevykdymo atliekant tarpvalstybinę operaciją.
3. Tapatumo nustatymo procedūrą vykdanči šalis atsako už tyčia ar dėl neatsargumo bet kuriam fiziniam arba juridiniam asmeniui padarytą žalą dėl 7 straipsnio f punkte nurodyto tinkamo tapatumo nustatymo vykdymo neužtikrinimo atliekant tarpvalstybinę operaciją.
4. 1, 2 ir 3 dalys taikomos laikantis nacionalinių atsakomybę reglamentuojančių taisyklių.
5. 1, 2 ir 3 dalys nedaro poveikio operacijos, kuriai naudojamos elektroninės atpažinties priemonės, kurioms taikoma elektroninės atpažinties schema, apie kurią pranešta pagal 9 straipsnio 1 dalį, šalių atsakomybei pagal nacionalinę teisę.

#### 12 straipsnis

##### Bendradarbiavimas ir sąveikumas

1. Nacionalinės elektroninės atpažinties schemos, apie kurias pranešta pagal 9 straipsnio 1 dalį, turi būti sąveikios.
2. 1 dalies tikslais nustatoma sąveikumo sistema.



3. Sąveikumo sistema turi atitikti šiuos kriterijus:

- a) ja siekiama būti neutralia technologiniu požiūriu ir ja nediskriminuojami jokie konkretūs nacionaliniai elektroninės atpažinties techniniai sprendimai valstybėje narėje;
- b) jei įmanoma, ji atitinka Europos ir tarptautinius standartus;
- c) ja sudaromos palankios sąlygos įgyvendinti projektuojant numatytos privatumo apsaugos principą; ir
- d) ja užtikrinama, kad asmens duomenys būtų tvarkomi pagal Direktyvą 95/46/EB.

4. Sąveikumo sistemą sudaro:

- a) nuoroda į minimalius techninius reikalavimus, susijusius su 8 straipsnyje numatytais saugumo užtikrinimo lygiais;
- b) elektroninės atpažinties schemų, apie kurias pranešta, nacionalinių saugumo užtikrinimo lygių suderinimas su 8 straipsnyje numatytais saugumo užtikrinimo lygiais;
- c) nuoroda į minimalius techninius sąveikumo reikalavimus;
- d) nuoroda į minimalų asmens tapatybės duomenų, kuriais nurodomas konkretus fizinis ar juridinis asmuo, rinkinį, prieinamą pasitelkiant elektroninės atpažinties schemas;
- e) darbo tvarkos taisyklės;
- f) ginčų sprendimo tvarka; ir
- g) bendri veiklos saugumo standartai.

5. Valstybės narės bendradarbiauja šiais klausimais:

- a) dėl elektroninės atpažinties schemų, apie kurias pranešta pagal 9 straipsnio 1 dalį, ir elektroninės atpažinties schemų, apie kurias valstybės narės ketina pranešti, sąveikumo ir
- b) dėl elektroninės atpažinties schemų saugumo.

6. Valstybių narių bendradarbiavimą sudaro:

- a) keitimasis informacija, patirtimi ir gerąja praktika, susijusiomis su elektroninės atpažinties schemomis, ir visų pirma su techniniais reikalavimais, susijusiais su sąveikumu ir saugumo užtikrinimo lygiais;
- b) keitimasis informacija, patirtimi ir gerąja praktika, susijusiomis su darbu taikant 8 straipsnyje numatytus elektroninės atpažinties schemų saugumo užtikrinimo lygius;
- c) elektroninės atpažinties schemų, kurioms taikomas šis reglamentas, tarpusavio vertinimas, ir
- d) atitinkamų pokyčių elektroninės atpažinties sektoriuje nagrinėjimas.

7. Ne vėliau kaip 2015 m. kovo 18 d. Komisija priima įgyvendinimo aktus, kuriais nustato procedūrinės sąlygas, būtinas sudaryti palankesnes 5 ir 6 dalyse nurodytu valstybių narių bendradarbiavimo sąlygas, siekiant skatinti aukštą pasitikėjimo lygį ir rizikos laipsnį atitinkantį saugumą.

8. Siekiant nustatyti vienodas 1 dalyje nustatyto reikalavimo įgyvendinimo sąlygas, ne vėliau kaip 2015 m. rugsėjo 18 d. Komisija, remdamasi 3 dalyje nustatytais kriterijais ir atsižvelgdama į valstybių narių bendradarbiavimo rezultatus, priima įgyvendinimo aktus dėl 4 dalyje įtvirtintos sąveikumo sistemos.

9. Šio straipsnio 7 ir 8 dalyse nurodyti įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

### III SKYRIUS

#### PATIKIMUMO UŽTIKRINIMO PASLAUGOS

##### 1 SKIRSNIS

##### **Bendrosios nuostatos**

##### 13 straipsnis

##### **Atsakomybė ir įrodinėjimo pareiga**

1. Nedarant poveikio 2 daliai, 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 prezumuojami, nebent kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas įrodo, kad pirmoje pastraipoje nurodyta žala padaryta nesant to kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo tyčios ar neatsargumo.

2. Kai patikimumo užtikrinimo paslaugų teikėjai iš anksto tinkamai informuoja savo klientus apie naudojimosi jų teikiamomis paslaugomis apribojimus ir kai tie apribojimai trečiosioms šalims yra atpažįstami, patikimumo užtikrinimo paslaugų teikėjai neatsako už žalą, padarytą naudojantis paslaugomis viršijant nurodytus apribojimus.

3. 1 ir 2 dalys taikomos laikantis nacionalinių atsakomybę reglamentuojančių taisyklių.

##### 14 straipsnis

##### **Tarptautiniai aspektai**

1. Trečiojoje valstybėje įsisteigusių patikimumo užtikrinimo paslaugų teikėjų 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, yra pripažįstamos pagal Sąjungos ir atitinkamos trečiosios valstybės arba tarptautinės organizacijos susitarimą pagal SESV 218 straipsnį.

2. 1 dalyje nurodytais susitarimais užtikrinama, visų pirma, kad:
- trečiųjų valstybių arba tarptautinių organizacijų, su kuriomis sudaryti susitarimai, patikimumo užtikrinimo paslaugų teikėjai laikytųsi Sąjungoje įsisteigusiems kvalifikuotiems patikimumo užtikrinimo paslaugų teikėjams ir jų teikiamoms kvalifikuotoms patikimumo užtikrinimo paslaugoms taikomų reikalavimų;
  - 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.

#### 15 straipsnis

#### **Neįgaliųjų galimybės**

Kai įmanoma, neįgaliesiems turi sudaroma galimybė naudotis teikiamomis patikimumo užtikrinimo paslaugomis ir teikiant tas paslaugas naudojamais galutinio vartojimo produktais.

#### 16 straipsnis

#### **Sankcijos**

Valstybės narės nustato sankcijų, taikytinų už šio reglamento pažeidimus, taisykles. Numatytos sankcijos turi būti veiksmingos, proporcingos ir atgrasančios.

#### 2 SKIRSNIS

#### **Priežiūra**

#### 17 straipsnis

#### **Priežiūros įstaiga**

1. Valstybės narės paskiria jų teritorijoje įsteigtą priežiūros įstaigą arba, abipusiu sutarimu su kita valstybe nare, toje kitoje valstybėje narėje įsteigtą priežiūros įstaigą. Ta įstaiga atsako už priežiūros funkcijų vykdymą paskiriančiojoje valstybėje narėje.

Priežiūros įstaigoms suteikiami būtini įgaliojimai ir pakankamai išteklių jų funkcijoms vykdyti.

- Valstybės narės praneša Komisijai atitinkamų jų paskirtų priežiūros įstaigų pavadinimus ir adresus.
- Priežiūros įstaigos vaidmuo:
  - priziūrėti paskiriančiosios valstybės narės teritorijoje įsisteigusių kvalifikuotus patikimumo užtikrinimo paslaugų teikėjus siekiant *ex ante* ir *ex post* priežiūros veikla užtikrinti, kad tie patikimumo užtikrinimo paslaugų teikėjai ir jų teikiamos kvalifikuotos patikimumo užtikrinimo paslaugos atitiktų šiame reglamente nustatytus reikalavimus;
  - vykdant *ex post* priežiūros veiklą, prireikus imtis veiksmų dėl paskiriančiosios valstybės narės teritorijoje įsisteigusių nekvalifikuotų patikimumo užtikrinimo paslaugų teikėjų, kai pranešama, kad tie nekvalifikuoti patikimumo užtikrinimo paslaugų teikėjai ar jų teikiamos patikimumo užtikrinimo paslaugos tariamai neatitinka šiame reglamente nustatytų reikalavimų.

4. Taikant 3 dalį ir laikantis joje numatytų apribojimų, priežiūros įstaigos funkcijos yra visų pirma:
- a) bendradarbiauti su kitomis priežiūros įstaigomis ir teikti joms pagalbą pagal 18 straipsnį;
  - b) analizuoti 20 straipsnio 1 dalyje ir 21 straipsnio 1 dalyje nurodytas atitikties įvertinimo ataskaitas;
  - c) informuoti kitas priežiūros įstaigas ir visuomenę apie saugumo ar vientisumo pažeidimus pagal 19 straipsnio 2 dalį;
  - d) vadovaujantis šio straipsnio 6 dalimi, teikti Komisijai ataskaitas apie savo pagrindinę veiklą;
  - e) vykdyti auditą arba reikalauti, kad atitikties vertinimo įstaiga atliktų kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų atitikties vertinimą pagal 20 straipsnio 2 dalį;
  - f) bendradarbiauti su duomenų apsaugos institucijomis, visų pirma, nepagrįstai nedelsiant jas informuojant apie kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų audito rezultatus kai tikėtina, kad buvo pažeistos asmens duomenų apsaugos taisyklės;
  - g) patikimumo užtikrinimo paslaugų teikėjams ir jų teikiamoms paslaugoms suteikti kvalifikacijos statusą ir jį panaikinti pagal 20 ir 21 straipsnius;
  - h) pranešti 22 straipsnio 3 dalyje nurodytai už nacionalinį patikimą sąrašą atsakingai įstaigai apie savo sprendimus suteikti arba panaikinti kvalifikacijos statusą, nebent ta įstaiga taip pat būtų priežiūros įstaiga;
  - i) patikrinti, ar priimtose ir teisingai taikomos nuostatos dėl nutraukimo planų tais atvejais, kai kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai nutraukia savo veiklą, be kita ko, patikrinti, kaip informacija laikoma prieinama pagal 24 straipsnio 2 dalies h punktą;
  - j) reikalauti, kad patikimumo užtikrinimo paslaugų teikėjai ištaisytų šiame reglamente nustatytų reikalavimų vykdymo pažeidimus.
5. Valstybės narės gali reikalauti, kad priežiūros įstaiga, laikydamosi nacionalinėje teisėje nustatytų sąlygų, sukurtų, tvarkytų ir atnaujintų patikimumo užtikrinimo infrastruktūrą.
6. Kiekviena priežiūros įstaiga kasmet ne vėliau kaip kovo 31 d. pateikia Komisijai ataskaitą apie praėjusiais kalendoriniais metais vykdytą pagrindinę veiklą kartu su pranešimu apie pažeidimus, gautų iš patikimumo užtikrinimo paslaugų teikėjų pagal 19 straipsnio 2 dalį, suvestine.
7. Komisija pateikia valstybėms narėms 6 dalyje nurodytą metinę ataskaitą.
8. Komisija gali priimti įgyvendinimo aktus, kuriais apibrėžia 6 dalyje nurodytos ataskaitos teikimo formatus ir procedūras. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

*18 straipsnis***Savitarpio pagalba**

1. Priežiūros įstaigos bendradarbiauja, siekdamos keistis gerąja praktika.

Priežiūros įstaiga, gavusi pagrįstą kitos priežiūros įstaigos prašymą, suteikia tai įstaigai pagalbą, kad priežiūros įstaigų veikla būtų vykdoma nuosekliai. Savitarpio pagalba visų pirma gali apimti informacijos prašymus ir priežiūros priemones, kaip antai prašymus atlikti patikras, susijusias su 20 ir 21 straipsniuose nurodytomis atitikties įvertinimo ataskaitomis.

2. Priežiūros įstaiga, kuriai teikiamas pagalbos prašymas, gali atsakyti patenkinti tą prašymą esant kuriam nors iš šių pagrindų:

- a) priežiūros įstaiga nėra kompetentinga suteikti prašomą pagalbą;
- b) prašoma pagalba nėra proporcinga priežiūros įstaigos priežiūros veiklai, vykdomai pagal 17 straipsnį;
- c) prašomos pagalbos suteikimas būtų nesuderinamas su šiuo reglamentu.

3. Prireikus valstybės narės gali atitinkamoms savo priežiūros įstaigoms leisti atlikti bendrus tyrimus, kuriuose dalyvautų kitų valstybių narių priežiūros įstaigų darbuotojai. Dėl tokių bendrų veiksmų tvarkos ir procedūrų susitaria ir jas nustato atitinkamos valstybės narės, laikydamosi savo nacionalinės teisės aktų.

*19 straipsnis***Patikimumo užtikrinimo paslaugų teikėjams keliami saugumo reikalavimai**

1. Kvalifikuoti ir nekvalifikuoti patikimumo užtikrinimo paslaugų teikėjai imasi reikiamų techninių ir organizacinių priemonių, kad būtų valdoma rizika, kylanti jų teikiamų patikimumo užtikrinimo paslaugų saugumui. Atsižvelgiant į naujausius technologinius pokyčius, tomis priemonėmis užtikrinama, kad saugumo lygis atitiktų rizikos lygį. Visų pirma imamasi priemonių, kad būtų išvengta saugumo incidentų, jog būtų kuo labiau sumažintas jų poveikis ir kad suinteresuotieji subjektai būtų informuoti apie neigiamą tokių incidentų poveikį.

2. Kvalifikuoti ir nekvalifikuoti patikimumo užtikrinimo paslaugų teikėjai, nepagrįstai nedelsdami, ir bet kuriuo atveju per 24 valandas nuo to momento, kai apie tai sužino, praneša priežiūros įstaigai ir, prireikus, kitoms atitinkamoms įstaigoms, kaip antai informacijos saugumo klausimais kompetentingai nacionalinei įstaigai arba duomenų apsaugos institucijai, apie visus saugumo arba vientisumo pažeidimus, turėjusius didelį poveikį teikiamai patikimumo užtikrinimo paslaugai arba ją teikiant naudojamiems asmens duomenims.

Kai saugumo ar vientisumo pažeidimas galėtų turėti neigiamo poveikio fiziniam ar juridiniam asmeniui, kuriam teikiama patikimumo užtikrinimo paslauga, patikimumo užtikrinimo paslaugų teikėjas taip pat nepagrįstai nedelsdamas praneša apie saugumo ar vientisumo pažeidimą tam fiziniam ar juridiniam asmeniui.

Prireikus – visų pirma, kai saugumo arba vientisumo pažeidimas yra susijęs su dviem arba daugiau valstybių narių – pranešimą gavusi priežiūros įstaiga informuoja kitų atitinkamų valstybių narių priežiūros įstaigas ir ENISA.

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.

3. Priežiūros įstaiga kartą per metus pateikia ENISA iš patikimumo užtikrinimo paslaugų teikėjų gautų pranešimų apie saugumo ar vientisumo pažeidimus suvestinę.



4. Komisija gali priimti įgyvendinimo aktus, kuriais:

- a) tiksliau apibrėžia 1 dalyje nurodytas priemones ir
- b) apibrėžia formatus ir procedūras, įskaitant terminus, taikytinus 2 dalies tikslais.

Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

### 3 SKYRIUS

#### **Kvalifikuotos patikimumo užtikrinimo paslaugos**

##### 20 straipsnis

#### **Kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų priežiūra**

1. Atitikties vertinimo įstaiga atlieka kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų auditą jų lėšomis bent kas 24 mėnesius. Audito tikslas – patvirtinti, kad kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai ir jų teikiamos kvalifikuotos patikimumo užtikrinimo paslaugos atitinka šiame reglamente nustatytus reikalavimus. Kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai po to parengtą atitikties įvertinimo ataskaitą priežiūros įstaigai pateikia per trijų darbo dienų laikotarpį nuo jos gavimo dienos.

2. Nedarant poveikio 1 daliai, priežiūros įstaiga gali bet kuriuo metu atlikti kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų auditą arba reikalauti, kad atitikties vertinimo įstaiga atliktų jų atitikties įvertinimą tų patikimumo užtikrinimo paslaugų teikėjų lėšomis, siekiant patvirtinti, kad jie ir jų teikiamos kvalifikuotos patikimumo užtikrinimo paslaugos atitinka šiame reglamente nustatytus reikalavimus. Kai nustatoma, kad buvo pažeistos asmens duomenų apsaugos taisyklės, priežiūros įstaiga praneša duomenų apsaugos institucijoms savo atliktų auditų rezultatus.

3. Kai priežiūros įstaiga reikalauja, kad kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas ištaisytų bet kurias šiame reglamente nustatytų reikalavimų vykdymo pažeidimus ir kai tas teikėjas to nepadaro, jei taikytina, per priežiūros įstaigos nustatytą laikotarpį, priežiūros įstaiga, atsižvelgdama visų pirma į tokių pažeidimų mastą, trukmę ir pasekmes, gali panaikinti to teikėjo arba pažeidimo paveiktų jo teikiamų paslaugų kvalifikacijos statusą ir pranešti apie tai 22 straipsnio 3 dalyje nurodytai įstaigai, kad būtų galima atnaujinti 22 straipsnio 1 dalyje nurodytus patikimumo sąrašus. Priežiūros įstaiga informuoja kvalifikuotą patikimumo užtikrinimo paslaugų teikėją apie jo kvalifikacijos statuso arba atitinkamos paslaugos kvalifikacijos statuso panaikinimą.

4. Komisija gali priimti įgyvendinimo aktus, kuriais nustato toliau nurodytų standartų referencinius numerius:

- a) atitikties vertinimo įstaigų akreditavimo ir 1 dalyje nurodytos atitikties vertinimo ataskaitos;
- b) audito taisyklių, pagal kurias atitikties vertinimo įstaigos atliks 1 dalyje nurodytą kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų atitikties vertinimą.

Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

*21 straipsnis***Kvalifikuotos patikimumo užtikrinimo paslaugos inicijavimas**

1. Kai kvalifikacijos statuso neturintys patikimumo užtikrinimo paslaugų teikėjai ketina pradėti teikti kvalifikuotas patikimumo užtikrinimo paslaugas, jie priežiūros įstaigai pateikia pranešimą apie savo ketinimą kartu su atitiktis vertinimo įstaigos parengta atitiktis įvertinimo ataskaita.

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

Jei priežiūros įstaiga padaro išvadą, kad patikimumo užtikrinimo paslaugų teikėjas ir jo teikiamos patikimumo užtikrinimo paslaugos atitinka pirmoje pastraipoje nurodytus reikalavimus, priežiūros įstaiga jam suteikia 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, nurodama vėlavimo priežastis ir laikotarpį, per kurį patikrinimas bus baigtas.

3. Kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai gali pradėti teikti kvalifikuotas patikimumo užtikrinimo paslaugas po to, kai kvalifikuotas statusas nurodomas patikimuose sąrašuose, nurodytuose 22 straipsnio 1 dalyje.

4. Komisija gali priimti įgyvendinimo aktus, kuriais apibrėžia formatus ir procedūras 1 ir 2 dalių tikslais. Tie įgyvendinimo aktai priimami pagal 48 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.

*22 straipsnis***Patikimi sąrašai**

1. Kiekviena valstybė narė sudaro, tvarko ir skelbia patikimus sąrašus, įskaitant informaciją apie kvalifikuotus patikimumo užtikrinimo paslaugų teikėjus, už kuriuos ji atsako, ir apie jų teikiamas kvalifikuotas patikimumo užtikrinimo paslaugas.

2. Valstybės narės sudaro, tvarko ir saugiai skelbia 1 dalyje nurodytus elektroniniu būdu pasirašytus arba užantspauduotus patikimus sąrašus, pateikdama juos tokia forma, kad juos būtų galima tvarkyti automatizuotomis priemonėmis.

3. Valstybės narės nepagrįstai nedelsdamos, pateikia Komisijai informaciją apie įstaigą, atsakingą už nacionalinių patikimų sąrašų sudarymą, tvarkymą ir skelbimą, ir išsamius duomenis apie tai, kur tokie sąrašai skelbiami, apie sertifikatus, naudojamus patikimiams sąrašams pasirašyti arba jiems patvirtinti spaudu, ir apie šios informacijos pasikeitimus.

4. Komisija saugiu ryšių kanalu visuomenei pateikia 3 dalyje numatytą elektroniniu būdu pasirašytą arba užantspauduotą informaciją tokia forma, kad ją būtų galima tvarkyti automatizuotomis priemonėmis.

5. Ne vėliau kaip 2015 m. rugsėjo 18 d. Komisija priima įgyvendinimo aktus, kuriais patikslina 1 dalyje nurodytą informaciją ir apibrėžia patikimų sąrašų technines specifikacijas ir formatus, taikytinus 1–4 dalių tikslais. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

## 23 straipsnis

**Kvalifikuotų patikimumo užtikrinimo paslaugų ES pasitikėjimo ženklas**

1. Po to, kai 21 straipsnio 2 dalies antroje pastraipoje nurodytas kvalifikacijos statusas nurodomas 22 straipsnio 1 dalyje nurodytuose patikimuose sąrašuose, kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai gali naudoti ES pasitikėjimo ženklą paprastai, atpažįstamai ir aiškiai žymėti savo teikiamas kvalifikuotas patikimumo užtikrinimo paslaugas.

2. Naudodami ES pasitikėjimo ženklą 1 dalyje nurodytoms kvalifikuotoms patikimumo užtikrinimo paslaugoms, kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai užtikrina, kad jų interneto svetainėje būtų pateikta nuoroda į atitinkamą patikimą sąrašą.

3. Ne vėliau kaip 2015 m. liepos 1 d. Komisija priima įgyvendinimo aktus, nustatančius specifikaciją, susijusią su forma, ir visų pirma su ES pasitikėjimo ženklo, skirto kvalifikuotoms patikimumo užtikrinimo paslaugoms, pateikimu, sandara, dydžiu ir dizainu. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

## 24 straipsnis

**Kvalifikuotiems patikimumo užtikrinimo paslaugų teikėjams keliami reikalavimai**

1. Išduodamas kvalifikuotą patikimumo užtikrinimo paslaugos sertifikatą, kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas tinkamomis priemonėmis pagal nacionalinės teisės aktus patikrina fizinio ar juridinio asmens, kuriam išduodamas kvalifikuotas sertifikatas, tapatybę ir, jeigu taikytina, visus jo specifinius požymius.

Pirmoje pastraipoje nurodytą informaciją kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, tikrina tiesiogiai arba patikėdamas tą atlikti trečiajai šaliai pagal nacionalinę teisę:

- a) fiziškai dalyvaujant fiziniam asmeniui arba juridinio asmens įgaliotajam atstovui; arba
- b) nuotoliniu būdu, naudodamas elektroninės atpažinties priemones, jei prieš išduodant kvalifikuotą sertifikatą jų atžvilgiu buvo užtikrintas fizinio ar juridinio asmens įgaliotojo atstovo fizinis dalyvavimas, ir kurios atitinka 8 straipsnyje nustatytus „pakankamo“ ir „aukšto“ saugumo užtikrinimo lygių reikalavimus; arba
- c) naudodamas pagal a arba b punktą išduotą kvalifikuotą elektroninio parašo arba elektroninio spaudo sertifikatą, arba
- d) naudodamas kitus nacionaliniu lygiu pripažintus tapatybės nustatymo būdus, kuriais užtikrinamas fiziniam dalyvavimui lygiavertis saugumo užtikrinimas. Lygiavertį saugumo užtikrinimą turi patvirtinti atitikties vertinimo įstaiga.

2. Kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, teikiantis kvalifikuotas patikimumo užtikrinimo paslaugas:

- a) informuoja priežiūros įstaigą apie bet kokius savo kvalifikuotų patikimumo užtikrinimo paslaugų teikimo pakeitimus ir ketinimą nutraukti tą veiklą;
- b) samdo darbuotojus ir, jei taikytina, subrangovus, kurie turi būtinos kompetencijos, yra patikimi, turi būtinos patirties ir kvalifikacijos, yra tinkamai apmokyti saugumo ir asmens duomenų apsaugos taisyklių, ir taiko Europos arba tarptautinius standartus atitinkančias administracines bei valdymo procedūras;
- c) atsakomybės už žalą rizikos atžvilgiu pagal 13 straipsnį, disponuoja pakankamais finansiniais ištekliais ir (arba) gauna tinkamą atsakomybės draudimą pagal nacionalinės teisės aktus;

- d) prieš užmezgdamas sutartinius santykius, aiškiai ir išsamiai informuoja visus asmenis, kurie nori naudotis kvalifikuota patikimumo užtikrinimo paslauga, apie tikslias naudojimosi ta paslauga sąlygas, įskaitant bet kokius naudojimosi ja apribojimus;
- e) naudoja patikimas sistemas ir produktus, kurie yra apsaugoti nuo pakeitimų, ir užtikrina jų palaikomo proceso techninį saugumą ir patikimumą;
- f) jam pateiktus duomenis patikrinama forma saugo patikimose sistemose, kad:
- i) juos būtų galima viešai gauti tik gavus asmens, su kuriuo yra susiję šie duomenys, sutikimą;
  - ii) saugomų duomenų įrašus ir pakeitimus galėtų daryti tik įgalioti asmenys;
  - iii) būtų galima patikrinti duomenų tikrumą;
- g) imasi tinkamų apsaugos nuo duomenų klastojimo ir vagystės priemonių;
- h) tinkamą laikotarpį, įskaitant kvalifikuotam patikimumo užtikrinimo paslaugų teikėjui nutraukus veiklą, registruoja ir laiko prieinama visą susijusią informaciją dėl kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo parengtų ir gautų duomenų, visų pirma tam, kad šią informaciją būtų galima panaudoti teismo procese kaip įrodymą ir siekiant užtikrinti paslaugų tęstinumą. Tokia informacija gali būti registruojama elektroniniu būdu;
- i) turi atnaujinamą nutraukimo planą, kad užtikrintų paslaugų tęstinumą, atsižvelgdami į priežiūros įstaigos pagal 17 straipsnio 4 dalies i punktą patikrintas nuostatas;
- j) užtikrina teisėtą asmens duomenų tvarkymą pagal Direktyvą 95/46/EB;
- k) tais atvejais, kai kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai išduoda kvalifikuotus sertifikatus – sukuria ir atnaujina sertifikatų duomenų bazę.

3. Jei kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, išduodantis kvalifikuotus sertifikatus nusprendžia atšaukti sertifikatą, tokį atšaukimą jis užregistruoja savo sertifikatų duomenų bazėje ir laiku paskelbia apie sertifikato atšaukimo statusą, ir bet kuriuo atveju per 24 valandas po prašymo gavimo dienos. Atšaukimas įsigalioja nedelsiant po jo paskelbimo.

4. Atsižvelgdami į 3 dalį, kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai, išduodantys kvalifikuotus sertifikatus, kiekvienai pasikliaujančiajai šaliai pateikia informaciją apie jų išduotų kvalifikuotų sertifikatų galiojimą arba atšaukimą. Ši informacija bet kuriuo metu, net ir pasibaigus sertifikato galiojimo laikotarpiui, pateikiama bent apie kiekvieną sertifikatą taikant automatizuotą būdą, kuris yra saugus, nemokamas ir veiksmingas.

5. Komisija gali priimti įgyvendinimo aktus, kuriais nustato patikimumo sistemoms ir produktams, kurie atitinka šio straipsnio 2 dalies e ir f punktų reikalavimus, taikomų standartų referencinius numerius. Jeigu patikimos sistemos ir produktai atitinka tuos standartus, laikoma, kad užtikrinta atitiktis šio straipsnio reikalavimams. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

## 4 SKIRSNIS

**Elektroniniai parašai**

## 25 straipsnis

**Elektroninių parašų teisinė galia**

1. Negalima atsisakyti pripažinti elektroninio parašo teisinės galios ir jo tinkamumo naudoti kaip įrodymą teismo procese tik dėl to, kad parašas yra elektroninis arba kad jis neatitinka kvalifikuoto elektroninių parašų reikalavimų.
2. Kvalifikuoto elektroninio parašo teisinė galia yra lygiavertė rašytiniam parašui.
3. Kvalifikuotas elektroninis parašas, patvirtintas vienoje valstybėje narėje išduotu kvalifikuotu sertifikatu, visose kitose valstybėse narėse pripažįstamas kaip kvalifikuotas elektroninis parašas.

## 26 straipsnis

**Pažangiojo elektroninio parašo reikalavimai**

Pažangusis elektroninis parašas turi atitikti toliau išvardytus reikalavimus:

- a) būti vienareikšmiškai susietas su pasirašančiu asmeniu;
- b) pagal jį galima nustatyti pasirašančio asmens tapatybę;
- c) sukurtas naudojant elektroninio parašo kūrimo duomenis, kuriuos tik pats pasirašantis asmuo gali labai patikimai naudoti; ir
- d) susietas su juo pasirašytais duomenimis taip, kad bet koks tų duomenų pakeitimas būtų pastebimas.

## 27 straipsnis

**Elektroniniai parašai viešųjų paslaugų srityje**

1. Jei valstybė narė pažangiojo elektroninio parašo reikalauja tam, kad būtų galima pasinaudoti viešojo sektoriaus įstaigos arba jos vardu teikiama internetine paslauga, ta valstybė narė pripažįsta pažangiuosius elektroninius parašus, kvalifikuotais elektroninių parašų sertifikatais patvirtintus pažangiuosius elektroninius parašus ir kvalifikuotus elektroninius parašus, kurie būtų taikomi bent tokių formatų arba naudojant tokius metodus, kokie apibrėžti 5 dalyje nurodytuose įgyvendinimo aktuose.
2. Jei valstybė narė kvalifikuotu sertifikatu patvirtinto pažangiojo elektroninio parašo reikalauja tam, kad būtų galima pasinaudoti viešojo sektoriaus įstaigos arba jos vardu teikiama internetine paslauga, ta valstybė narė pripažįsta kvalifikuotais sertifikatais patvirtintus pažangiuosius elektroninius parašus ir kvalifikuotus elektroninius parašus, kurie būtų taikomi bent tokių formatų arba naudojant tokius metodus, kokie apibrėžti 5 dalyje nurodytuose įgyvendinimo aktuose.
3. Valstybės narės nereikalauja, kad tarpvalstybinio naudojimosi viešojo sektoriaus įstaigos teikiama internetine paslauga atveju būtų naudojamas elektroninis parašas, kurio saugumo užtikrinimo lygis būtų aukštesnis nei kvalifikuoto elektroninio parašo.
4. Komisija gali priimti įgyvendinimo aktus, kuriais nustato pažangiesiems elektroniniams parašams taikomų standartų referencinius numerius. Jeigu pažangusis elektroninis parašas atitinka tuos standartus, laikoma, kad užtikrinta atitiktis šio straipsnio 1 ir 2 dalyse ir 26 straipsnyje pažangiesiems elektroniniams parašams nustatytiems reikalavimams. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

5. Ne vėliau kaip 2015 m. rugsėjo 18 d. Komisija, atsižvelgdama į taikomą praktiką, standartus ir Sąjungos teisės aktus, įgyvendinimo aktais apibrėžia pažangiųjų elektroninių parašų bazinius formatus arba bazinius metodus, kai naudojami alternatyvūs formatai. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

#### 28 straipsnis

##### **Kvalifikuoti elektroninių parašų sertifikatai**

1. Kvalifikuoti elektroninių parašų sertifikatai turi atitikti I priede nustatytus reikalavimus.
2. Kvalifikuotiems elektroninių parašų sertifikatams netaikoma jokių privalomų reikalavimų, viršijančių I priede nustatytus reikalavimus.
3. Kvalifikuoti elektroninių parašų sertifikatai gali turėti neprivalomų papildomų specifinių požymių. Tie požymiai nedaro poveikio kvalifikuotų elektroninių parašų sąveikumui ir pripažinimui.
4. Jeigu iš pradžių aktyvintas kvalifikuotas elektroninio parašo sertifikatas vėliau atšaukiamas, jis netenka galios nuo jo atšaukimo momento, o jo statuso jokiais aplinkybėmis negalima atkurti.
5. Valstybės narės gali nustatyti kvalifikuotų elektroninių parašų sertifikatų galiojimo laikino sustabdymo nacionalines taisykles, laikydamosi šių sąlygų:
  - a) jei kvalifikuoto elektroninio parašo sertifikato galiojimas buvo laikinai sustabdytas, tas sertifikatas netenka galios sustabdymo laikotarpiu;
  - b) galiojimo sustabdymo laikotarpis yra aiškiai nurodomas sertifikatų duomenų bazėje, o tai, kad sertifikato galiojimas yra sustabdytas, galiojimo sustabdymo laikotarpiu matoma teikiant informaciją apie sertifikato statusą.
6. Komisija gali priimti įgyvendinimo aktus, kuriais nustato kvalifikuotiems elektroninio parašo sertifikatams taikomų standartų referencinius numerius. Jeigu kvalifikuotas elektroninio parašo sertifikatas atitinka tuos standartus, laikoma, kad užtikrinta atitiktis I priede nustatytiems reikalavimams. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

#### 29 straipsnis

##### **Reikalavimai kvalifikuotiems elektroninio parašo kūrimo įtaisams**

1. Kvalifikuoti elektroninio parašo kūrimo įtaisai turi atitikti II priede nustatytus reikalavimus.
2. Komisija gali priimti įgyvendinimo aktus, kuriais nustato kvalifikuotiems elektroninio parašo kūrimo įtaisams taikomų standartų referencinius numerius. Jeigu kvalifikuotas elektroninio parašo kūrimo įtaisas atitinka tuos standartus, laikoma, kad užtikrinta atitiktis II priede nustatytiems reikalavimams. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

#### 30 straipsnis

##### **Kvalifikuotų elektroninio parašo kūrimo įtaisų sertifikavimas**

1. Kvalifikuotų elektroninio parašo kūrimo įtaisų atitiktį II priede nustatytiems reikalavimams sertifikuoja valstybių narių paskirtos atitinkamos viešosios ar privačiosios įstaigos.

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

3. 1 dalyje nurodytas sertifikavimas grindžiamas viena iš šių procedūrų:

a) saugumo vertinimo procedūra, atlikta pagal vieną iš informacinių technologijų produktų saugumo vertinimo standartų, įtrauktų į sąrašą nustatytą pagal antrą pastraipą, arba

b) kita nei a punkte nurodyta procedūra su sąlyga, kad joje taikomi panašūs saugumo lygiai, o 1 dalyje nurodyta viešoji ar privatioji įstaiga apie tą procedūrą praneša Komisijai. Ta procedūra gali būti taikoma tik tuo atveju, kai nėra a punkte nurodytų standartų arba kai tebevyksta a punkte nurodyta saugumo vertinimo procedūra.

Komisija priimdama įgyvendinimo aktus sudaro iš informacinių technologijų produktų, nurodytų a punkte, saugumo vertinimo standartų sąrašą. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

4. Komisijai pagal 47 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus dėl specialiųjų kriterijų, kuriuos turėtų atitikti šio straipsnio 1 dalyje nurodytos paskirtos įstaigos, nustatymo.

#### 31 straipsnis

##### **Sertifikuotų kvalifikuotų elektroninio parašo kūrimo įtaisų sąrašo skelbimas**

1. Valstybės narės nepagrįstai nedelsdamos ir ne vėliau kaip per vieną mėnesį po sertifikavimo užbaigimo dienos, pateikia Komisijai informaciją apie kvalifikuotus elektroninio parašo kūrimo įtaisus, kuriuos sertifikavo 30 straipsnio 1 dalyje nurodytos įstaigos. Be to, nepagrįstai nedelsdamos ir ne vėliau kaip per vieną mėnesį po sertifikavimo atšaukimo dienos, jos pateikia Komisijai informaciją apie elektroninio parašo kūrimo įtaisus, kurie nebebus sertifikuojami.

2. Remdamasi gauta informacija Komisija sudaro, skelbia ir prižiūri sertifikuotų kvalifikuotų elektroninio parašo kūrimo įtaisų sąrašą.

3. Komisija gali priimti įgyvendinimo aktus, kuriais apibrėžia formatus ir procedūras, taikytinus 1 dalies tikslais. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

#### 32 straipsnis

##### **Reikalavimai kvalifikuotų elektroninių parašų galiojimo patvirtinimui**

1. Kvalifikuoto elektroninio parašo galiojimo patvirtinimo procedūra patvirtinamas kvalifikuoto elektroninio parašo 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) elektroninis parašas sukurtas naudojant kvalifikuotą elektroninio parašo kūrimo įtaisą;
- g) nebuvo pažeistas pasirašytų duomenų vientisumas;
- h) pasirašymo metu buvo laikomasi 26 straipsnyje nurodytų reikalavimų.

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

3. Komisija gali priimti įgyvendinimo aktus, kuriais nustato kvalifikuotų elektroninių parašų galiojimo patvirtinimo standartų referencinius numerius. Jeigu kvalifikuotų elektroninių parašų galiojimo patvirtinimas atitinka tuos standartus, laikoma, kad užtikrinta atitiktis 1 dalyje nustatytiems reikalavimams. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

### 33 straipsnis

#### **Kvalifikuotų elektroninių parašų kvalifikuota galiojimo patvirtinimo paslauga**

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

- a) suteikia galiojimo patvirtinimą pagal 32 straipsnio 1 dalį, ir
- b) suteikia pasikliaujančiosioms šalims galimybę galiojimo patvirtinimo procedūros rezultatą gauti automatizuotu būdu, kuris būtų patikimas, veiksmingas ir susietas su kvalifikuotos galiojimo patvirtinimo paslaugos teikėjo pažangiuoju elektroniniu parašu arba pažangiuoju elektroniniu spaudu.

2. Komisija gali priimti įgyvendinimo aktus, kuriais nustato 1 dalyje nurodytoms kvalifikuotoms galiojimo patvirtinimo paslaugoms taikomų standartų referencinius numerius. Jeigu kvalifikuoto elektroninio parašo galiojimo patvirtinimo paslauga atitinka tuos standartus, laikoma, kad užtikrinta atitiktis 1 dalyje nustatytiems reikalavimams. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

### 34 straipsnis

#### **Kvalifikuotų elektroninių parašų kvalifikuota ilgalaikės apsaugos paslauga**

1. Kvalifikuotų elektroninių parašų kvalifikuotą ilgalaikės apsaugos 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. Komisija gali priimti įgyvendinimo aktus, kuriais nustato kvalifikuotų elektroninių parašų kvalifikuotos ilgalaikės apsaugos paslaugos standartų referencinius numerius. Jeigu kvalifikuotų elektroninių parašų kvalifikuotos ilgalaikės apsaugos paslaugos priemonės atitinka tuos standartus, laikoma, kad užtikrinta atitiktis 1 dalyje nustatytiems reikalavimams. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

## 5 SKIRSNIS

**Elektroniniai spaudai**

## 35 straipsnis

**Elektroninio spaudo teisinė galia**

1. Negalima atsisakyti pripažinti elektroninio spaudo teisinės galios ir jo tinkamumo naudoti kaip įrodymą teismo procese tik dėl to, kad spaudas yra elektroninis arba kad jis neatitinka kvalifikuotų elektroninių spaudų reikalavimų.
2. Kvalifikuotam elektroniniam spaudui taikoma prezumpcija dėl duomenų, su kuriais susietas kvalifikuotas elektroninis spaudas, vientisumo ir tų duomenų kilmės tinkamumo.
3. Kvalifikuotas elektroninis spaudas, patvirtintas vienoje valstybėje narėje išduotu kvalifikuotu sertifikatu, visose kitose valstybėse narėse pripažįstamas kvalifikuotu elektroniniu spaudu.

## 36 straipsnis

**Reikalavimai pažangiesiems elektroniniams spaudams**

Pažangusis elektroninis spaudas turi atitikti toliau išvardytus reikalavimus:

- a) jis turi būti vienareikšmiškai susietas su spaudo kūrėju;
- b) pagal jį galima nustatyti spaudo kūrėjo tapatybę;
- c) jis turi būti sukurtas naudojant elektroninio spaudo kūrimo duomenis, kuriuos spaudo kūrėjas gali labai patikimai pats naudoti kurdamas elektroninį spaudą, ir
- d) jis turi būti susietas su juo nurodomais duomenimis taip, kad būtų pastebimas bet koks vėlesnis tų duomenų pakeitimas.

## 37 straipsnis

**Elektroniniai spaudai viešųjų paslaugų srityje**

1. Jei valstybė narė pažangiojo elektroninio spaudo reikalauja tam, kad būtų galima pasinaudoti viešojo sektoriaus įstaigos arba jos vardu teikiama internetine paslauga, ta valstybė narė pripažįsta pažangiuosius elektroninius spaudus, kvalifikuotais elektroninių spaudų sertifikatais patvirtintus pažangiuosius elektroninius spaudus ir kvalifikuotus elektroninius spaudus, kurie būtų taikomi bent tokių formatų arba naudojant tokius metodus, kokie apibrėžti 5 dalyje nurodytuose įgyvendinimo aktuose.
2. Jei valstybė narė kvalifikuotu sertifikatu patvirtinto pažangiojo elektroninio spaudo reikalauja tam, kad būtų galima pasinaudoti viešojo sektoriaus įstaigos arba jos vardu teikiama internetine paslauga, ta valstybė narė pripažįsta kvalifikuotais sertifikatais patvirtintus pažangiuosius elektroninius spaudus ir kvalifikuotus elektroninius spaudus, kurie būtų taikomi bent tokių formatų arba naudojant tokius metodus, kokie apibrėžti 5 dalyje nurodytuose įgyvendinimo aktuose.
3. Valstybės narės nereikalauja, kad norint tarpvalstybiniu lygiu pasinaudoti viešojo sektoriaus įstaigos teikiama internetine paslauga būtų naudojamas elektroninis spaudas, kurio saugumo užtikrinimo lygis būtų aukštesnis nei kvalifikuoto elektroninio spaudo.
4. Komisija gali priimti įgyvendinimo aktus, kuriais nustato pažangiesiems elektroniniams spaudams taikomų standartų referencinius numerius. Jeigu pažangusis elektroninis spaudas atitinka tuos standartus, laikoma, kad užtikrinta atitiktis šio straipsnio 1 ir 2 dalyse ir 36 straipsnyje pažangiesiems elektroniniams spaudams nustatytiems reikalavimams. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

5. Ne vėliau kaip 2015 m. rugsėjo 18 d. Komisija, atsižvelgdama į taikomą praktiką, standartus ir Sąjungos teisės aktus, įgyvendinimo aktais apibrėžia pažangiųjų elektroninių spaudų bazinius formatus arba bazinius metodus, kai naudojami alternatyvūs formatai. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

### 38 straipsnis

#### **Kvalifikuoti elektroninių spaudų sertifikatai**

1. Kvalifikuoti elektroninių spaudų sertifikatai turi atitikti III priede nustatytus reikalavimus.
2. Kvalifikuotiems elektroninių spaudų sertifikatams netaikoma jokių privalomų reikalavimų, viršijančių III priede nustatytus reikalavimus.
3. Kvalifikuoti elektroninių spaudų sertifikatai gali turėti neprivalomų papildomų specifinių požymių. Tie požymiai nedaro poveikio kvalifikuotų elektroninių spaudų sąveikumui ir pripažinimui.
4. Jeigu iš pradžių aktyvintas kvalifikuotas elektroninio spaudo sertifikatas vėliau atšaukiamas, jis netenka galios nuo jo atšaukimo momento, o jo statuso jokiais aplinkybėmis negalima atkurti.
5. Valstybės narės gali nustatyti kvalifikuotų elektroninių spaudų sertifikatų galiojimo laikino sustabdymo nacionalines taisykles, laikydamosi šių sąlygų:
  - a) jei kvalifikuoto elektroninio spaudo sertifikato galiojimas buvo laikinai sustabdytas, tas sertifikatas netenka galios sustabdymo laikotarpiu;
  - b) galiojimo sustabdymo laikotarpis yra aiškiai nurodomas sertifikatų duomenų bazėje ir tai, kad sertifikato galiojimas yra sustabdytas, galiojimo sustabdymo laikotarpiu matoma teikiant informaciją apie sertifikato statusą.
6. Komisija gali priimti įgyvendinimo aktus, kuriais nustato kvalifikuotiems elektroninio spaudo sertifikatams taikomų standartų referencinius numerius. Jeigu kvalifikuotas elektroninio spaudo sertifikatas atitinka tuos standartus, laikoma, kad užtikrinta atitiktis III priede nustatytiems reikalavimams. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

### 39 straipsnis

#### **Kvalifikuoti elektroninio spaudo kūrimo įtaisai**

1. Kvalifikuotiems elektroninio spaudo kūrimo įtaisams *mutatis mutandis* taikomi 29 straipsnyje nustatyti reikalavimai.
2. Kvalifikuotų elektroninio spaudo kūrimo įtaisų sertifikavimui *mutatis mutandis* taikomas 30 straipsnis.
3. Sertifikuotų kvalifikuotų elektroninio spaudo kūrimo įtaisų sąrašo skelbimui *mutatis mutandis* taikomas 31 straipsnis.

### 40 straipsnis

#### **Kvalifikuotų elektroninių spaudų galiojimo patvirtinimas ir ilgalaikė apsauga**

Kvalifikuotų elektroninių spaudų galiojimo patvirtinimui ir ilgalaikė apsaugai *mutatis mutandis* taikomi 32, 33 ir 34 straipsniai.

## 6 SKIRSNIS

**Elektroninė laiko žyma**

## 41 straipsnis

**Elektroninių laiko žymų teisinė galia**

1. Negalima atsisakyti pripažinti elektroninės laiko žymos teisinės galios ir jos tinkamumo naudoti kaip įrodymą teismo procese tik dėl to, kad žyma yra elektroninė arba kad ji neatitinka kvalifikuotoms elektroninėms laiko žymoms keliamų reikalavimų.
2. Kvalifikuotai elektronei laiko žymai taikoma prezumpcija dėl datos ir laiko, kurie joje nurodomi, tikslumo ir duomenų, su kuriais susieta data ir laikas, vientisumo.
3. Kvalifikuota elektroninė laiko žyma, išduota vienoje valstybėje narėje, pripažįstama kaip kvalifikuota elektroninė laiko žyma visose valstybėse narėse.

## 42 straipsnis

**Kvalifikuotoms elektroninėms laiko žymoms keliami reikalavimai**

1. Kvalifikuota elektroninė laiko žyma turi atitikti šiuos reikalavimus:
  - a) ji susieja datą ir laiką su duomenimis taip, kad pagrįstai neliktų galimybės nepastebimai pakeisti duomenų;
  - b) ji grindžiama tiksliu laiko šaltiniu, susietu su suderintuoju pasauliniu laiku, ir
  - c) ji pasirašyta naudojant kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo pažangųjį elektroninį parašą arba patvirtinta jo pažangiuoju elektroniniu spaudu arba lygiaverčiu būdu.
2. Komisija gali priimti įgyvendinimo aktus, kuriais nustato datos ir laiko susiejimo su duomenimis ir tikslų laiko šaltinių standartų referencinius numerius. Jeigu datos ir laiko susiejimas su duomenimis ir tikslus laiko šaltinis atitinka tuos standartus, laikoma, kad užtikrinta atitiktis 1 dalyje nustatytiems reikalavimams. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

## 7 SKIRSNIS

**Elektroninio registruoto pristatymo paslaugos**

## 43 straipsnis

**Elektroninio registruoto pristatymo paslaugų teisinė galia**

1. Negalima atsisakyti pripažinti naudojantis elektroninio registruoto pristatymo paslaugomis išsiųstų ir gautų duomenų teisinės galios ir jų tinkamumo naudoti kaip įrodymą teismo procese tik dėl to, kad jis yra elektroninis arba kad neatitinka kvalifikuotoms elektroninio registruoto pristatymo paslaugoms keliamų reikalavimų.
2. Naudojantis kvalifikuotomis elektroninio registruoto pristatymo paslaugomis išsiųstų ir gautų duomenų atveju preziumuojama, kad tie duomenys yra vientisi, duomenis išsiuntė siuntėjas ir juos gavo gavėjas, kurių tapatybės žinomos, o duomenų išsiuntimo ir gavimo data bei laikas, nurodyti naudojantis kvalifikuotomis elektroninio registruoto pristatymo paslaugomis, yra tikslūs.

## 44 straipsnis

**Kvalifikuotoms elektroninio registruoto pristatymo paslaugoms keliami reikalavimai**

1. Kvalifikuotos elektroninio registruoto pristatymo paslaugos turi atitikti šiuos reikalavimus:
  - a) jas teikia vienas arba daugiau kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas (-ai);
  - b) jos užtikrina galimybę labai patikimai nustatyti siuntėjo tapatybę;
  - c) jos turi užtikrinti, kad būtų nustatyta gavėjo tapatybė prieš duomenis pristatant;
  - d) duomenų siuntimas ir gavimas yra apsaugoti kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo pažangiuoju elektroniniu parašu arba pažangiuoju elektroniniu spaudu taip, kad neliktų galimybės nepastebimai pakeisti duomenų;
  - e) bet koks duomenų pakeitimas, būtinas norint išsiųsti arba gauti duomenis, aiškiai nurodomas duomenų siuntėjui ir gavėjui;
  - f) duomenų išsiuntimo, gavimo ir bet kokio duomenų pakeitimo data ir laikas yra nurodyti naudojant kvalifikuotą elektroninę laiko žymą.

Kai vienas ar daugiau kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų perduoda duomenis vienas kitam, a–f punktų reikalavimai taikomi visiems kvalifikuotiems patikimumo užtikrinimo paslaugų teikėjams.

2. Komisija gali priimti įgyvendinimo aktus, kuriais nustato duomenų siuntimo ir gavimo procesams taikomų standartų referencinius numerius. Jeigu duomenų siuntimo ir gavimo procesas atitinka tuos standartus, laikoma, kad užtikrinta atitiktis 1 dalyje nustatytiems reikalavimams. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

## 8 SKIRSNIS

**Interneto svetainės tapatumo nustatymas**

## 45 straipsnis

**Kvalifikuotiems interneto svetainės tapatumo nustatymo sertifikatams keliami reikalavimai**

1. Kvalifikuoti interneto svetainės tapatumo nustatymo sertifikatai turi atitikti IV priede nustatytus reikalavimus.
2. Komisija gali priimti įgyvendinimo aktus, kuriais nustato kvalifikuotiems interneto svetainės tapatumo nustatymo sertifikatams taikytinų standartų referencinius numerius. Jeigu kvalifikuotas interneto svetainės tapatumo nustatymo sertifikatas atitinka tuos standartus, laikoma, kad yra užtikrinta atitiktis IV priede nustatytiems reikalavimams. Tie įgyvendinimo aktai priimami laikantis 48 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

## IV SKYRIUS

**ELEKTRONINIAI DOKUMENTAI**

## 46 straipsnis

**Elektroninių dokumentų teisinė galia**

Negalima atsakyti pripažinti elektroninio dokumento teisinės galios ir jo tinkamumo naudoti kaip įrodymą teismo procese tik dėl to, kad jis yra elektroninis.

## V SKYRIUS

**ĮGALIOJIMŲ DELEGAVIMAS IR ĮGYVENDINIMO NUOSTATOS**

## 47 straipsnis

**Įgaliojimų delegavimas**

1. Įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami šiame straipsnyje nustatytais sąlygomis.
2. 30 straipsnio 4 dalyje nurodyti įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami neribotam laikotarpiui nuo 2014 m. rugsėjo 17 d.
3. Europos Parlamentas arba Taryba gali bet kada atšaukti 30 straipsnio 4 dalyje nurodytus deleguotuosius įgaliojimus. Sprendimu dėl įgaliojimų atšaukimo nutraukiami tame sprendime nurodyti įgaliojimai priimti deleguotuosius aktus. Sprendimas įsigalioja kitą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje* arba vėlesnę jame nurodytą dieną. Jis nedaro poveikio jau galiojančių deleguotųjų aktų galiojimui.
4. Apie priimtą deleguotąjį aktą Komisija nedelsdama vienu metu praneša Europos Parlamentui ir Tarybai.
5. Pagal 30 straipsnio 4 dalį priimtas deleguotasis aktas įsigalioja tik tuo atveju, jeigu per du mėnesius nuo pranešimo Europos Parlamentui ir Tarybai apie šį aktą dienos nei Europos Parlamentas, nei Taryba nepareiškia prieštaravimų arba jeigu dar nepasibaigus šiam laikotarpiui ir Europos Parlamentas, ir Taryba praneša Komisijai, kad prieštaravimų nereikš. Europos Parlamento arba Tarybos iniciatyva šis laikotarpis pratęsiamas dviem mėnesiais.

## 48 straipsnis

**Komiteto procedūra**

1. Komisijai padeda komitetas. Tas komitetas – tai komitetas, kaip nustatyta Reglamente (ES) Nr. 182/2011.
2. Kai daroma nuoroda į šią dalį, taikomas Reglamento (ES) Nr. 182/2011 5 straipsnis.

## VI SKYRIUS

**BAIGIAMOSIOS NUOSTATOS**

## 49 straipsnis

**Peržiūra**

Komisija atlieka šio reglamento taikymo peržiūrą ir pateikia Europos Parlamentui ir Tarybai ataskaitą ne vėliau kaip 2020 m. liepos 1 d. Komisija visų pirma įvertina, ar tinkama pakeisti šio reglamento taikymo sritį ar specifines jo nuostatas, įskaitant 6 straipsnį, 7 straipsnio f punktą, 34, 43, 44 ir 45 straipsnius, atsižvelgiant į taikant šį reglamentą įgytą patirtį, taip pat į technologinius, rinkos ir teisinius pokyčius.

Kartu su pirmoje pastraipoje nurodyta ataskaita prireikus pateikiami pasiūlymai dėl teisėkūros procedūra priimamų aktų.

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

## 50 straipsnis

**Panaikinimas**

1. Direktyva 1999/93/EB panaikinama nuo 2016 m. liepos 1 d.
2. Nuorodos į panaikintą direktyvą laikomos nuorodomis į šį reglamentą.

## 51 straipsnis

**Pereinamojo laikotarpio priemonės**

1. Pažangūs parašo kūrimo įtaisai, kurių atitikties buvo nustatyta pagal Direktyvos 1999/93/EB 3 straipsnio 4 dalį, pagal šį reglamentą laikomi kvalifikuotais elektroninio parašo kūrimo įtaisais.
2. Pagal Direktyvą 1999/93/EB fiziniams asmenims išduoti kvalifikuoti sertifikatai pagal šį reglamentą laikomi kvalifikuotais elektroninių parašų sertifikatais iki jų galiojimo pabaigos.
3. Kvalifikuotus sertifikatus pagal Direktyvą 1999/93/EB išduodantis sertifikavimo paslaugų teikėjas kuo greičiau, bet ne vėliau kaip 2017 m. liepos 1 d. priežiūros įstaigai pateikia atitikties įvertinimo ataskaitą. Kol nepateikiama tokia atitikties įvertinimo ataskaita ir priežiūros įstaiga baigia jos įvertinimą, tas sertifikavimo paslaugų teikėjas pagal šį reglamentą laikomas kvalifikuotu patikimumo užtikrinimo paslaugų teikėju.
4. Jei kvalifikuotus sertifikatus pagal Direktyvą 1999/93/EB išduodantis sertifikavimo paslaugų teikėjas per 3 dalyje nurodytą laikotarpį priežiūros įstaigai nepateikia atitikties įvertinimo ataskaitos, tas sertifikavimo paslaugų teikėjas pagal šį reglamentą nuo 2017 m. liepos 2 d. nelaikomas kvalifikuotu patikimumo užtikrinimo paslaugų teikėju.

## 52 straipsnis

**Įsigaliojimas**

1. Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.
2. Šis reglamentas taikomas nuo 2016 m. liepos 1 d., išskyrus:
  - a) 8 straipsnio 3 dalį, 9 straipsnio 5 dalį, 12 straipsnio 2–9 dalis, 17 straipsnio 8 dalį, 19 straipsnio 4 dalį, 20 straipsnio 4 dalį, 21 straipsnio 4 dalį, 22 straipsnio 5 dalį, 23 straipsnio 3 dalį, 24 straipsnio 5 dalį, 27 straipsnio 4 ir 5 dalis, 28 straipsnio 6 dalį, 29 straipsnio 2 dalį, 30 straipsnio 3 ir 4 dalis, 31 straipsnio 3 dalį, 32 straipsnio 3 dalį, 33 straipsnio 2 dalį, 34 straipsnio 2 dalį, 37 straipsnio 4 ir 5 dalis, 38 straipsnio 6 dalį, 42 straipsnio 2 dalį, 44 straipsnio 2 dalį, 45 straipsnio 2 dalį, 47 ir 48 straipsnius, kurie taikomi nuo 2014 m. rugsėjo 17 d.;
  - b) 7 straipsnį, 8 straipsnio 1 ir 2 dalis, 9 straipsnį, 10 straipsnį, 11 straipsnį, 12 straipsnio 1 dalį, kurie taikomi nuo 8 straipsnio 3 dalyje ir 12 straipsnio 8 dalyje nurodytų įgyvendinimo aktų taikymo pradžios dienos;
  - c) 6 straipsnį, kuris pradedamas taikyti praėjus trejiems metams nuo 8 straipsnio 3 dalyje ir 12 straipsnio 8 dalyje nurodytų įgyvendinimo aktų taikymo pradžios dienos.
3. Kai elektroninės atpažinties schema, apie kurią pranešta, įtraukiama į Komisijos pagal 9 straipsnį skelbiamą sąrašą iki šio straipsnio 2 dalies c punkte nurodytos datos, elektroninės atpažinties priemonių pagal tą schemą pripažinimas vadovaujantis 6 straipsniu atliekamas ne vėliau kaip per 12 mėnesių po to, kai paskelbiama apie tą schemą, tačiau ne anksčiau kaip šio straipsnio 2 dalies c punkte nurodytą datą.



4. Nepaisant šio straipsnio 2 dalies c punkto, valstybė narė gali nuspręsti, kad elektroninės atpažinties priemonės pagal elektroninės atpažinties schemą, apie kurią kita valstybė narė pranešė vadovaudamasi 9 straipsnio 1 dalimi, yra pripažįstamos pirmojoje valstybėje narėje nuo 8 straipsnio 3 dalyje ir 12 straipsnio 8 dalyje nurodytų įgyvendinimo aktų taikymo pradžios dienos. Atitinkamos valstybės narės informuoja Komisiją. Komisija šią informaciją skelbia viešai.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2014 m. liepos 23 d.

*Parlamento vardu*

*Pirmininkas*

M. SCHULZ

*Tarybos vardu*

*Pirmininkas*

S. GOZI

## I PRIEDAS

**KVALIFIKUOTIEMS ELEKTRONINIŲ PARAŠŲ SERTIFIKATAMS KELIAMI REIKALAVIMAI**

Kvalifikuotuose elektroninių parašų sertifikatuose pateikiama:

- a) nuoroda (bent tokia forma, kad ją būtų galima tvarkyti automatizuotomis priemonėmis), kad sertifikatas išduotas kaip kvalifikuotas elektroninio parašo sertifikatas;
  - b) duomenų rinkinys, kuriuo vienareikšmiškai nurodomas kvalifikuotas sertifikatus išduodantis kvalifikuotas patikimumo užtikrinimo paslaugų 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;
  - c) bent pasirašančio asmens vardas ir pavardė arba slapyvardis; jei naudojamas slapyvardis, tai aiškiai nurodoma;
  - d) elektroninio parašo patvirtinimo duomenys, atitinkantys elektroninio parašo kūrimo duomenis;
  - e) duomenys apie sertifikato galiojimo laikotarpio pradžią ir pabaigą;
  - f) sertifikato identifikacinis kodas, kuris turi būti unikalus kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo atžvilgiu;
  - g) sertifikatą išduodančio kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo pažangusis elektroninis parašas arba pažangusis elektroninis spaudas;
  - h) vieta, kurioje galima nemokamai gauti sertifikatą, patvirtinantį g punkte nurodytą pažangųjį elektroninį parašą arba pažangųjį elektroninį spaudą;
  - i) paslaugų teikimo vieta, kurioje galima pasiteirauti dėl kvalifikuoto sertifikato galiojimo;
  - j) jeigu elektroninio parašo kūrimo duomenys, susiję su elektroninio parašo patvirtinimo duomenimis, yra kvalifikuotame elektroninio parašo kūrimo įtaise, atitinkama tai nurodanti informacija pateikiama bent tokia forma, kad ją būtų galima tvarkyti automatizuotomis priemonėmis.
-

## II PRIEDAS

**KVALIFIKUOTIEMS ELEKTRONINIO PARAŠO KŪRIMO ĮTAISAMS KELIAM REIKALAVIMAI**

1. Kvalifikuotais elektroninio parašo kūrimo įtaisais, taikant atitinkamas technines ir procedūrines priemones, užtikrinama bent tiek, 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 pašalinta kuriant elektroninį parašą naudojamų elektroninio parašo kūrimo duomenų išvedimo 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 nekeičiami pasirašomi duomenys arba netrukdoma pateikti šių duomenų pasirašančiam asmeniui prieš pasirašymą.
  3. Elektroninio parašo kūrimo duomenis pasirašančio asmens vardu gali rengti arba tvarkyti tik kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas.
  4. Nedarant poveikio 1 punkto d papunkčiui, kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai, pasirašančio asmens vardu tvarkantys elektroninio parašo kūrimo duomenis, gali daryti atsargines elektroninio parašo kūrimo duomenų kopijas tik duomenims atkurti, jeigu laikomasi šių reikalavimų:
    - a) duomenų rinkinių kopijų saugumo lygis turi būti toks pat kaip originalių duomenų rinkinių;
    - b) duomenų rinkinių kopijų negali būti daugiau nei būtina norint užtikrinti paslaugos tęstinumą.
-

## III PRIEDAS

**KVALIFIKUOTIEMS ELEKTRONINIŲ SPAUDŲ SERTIFIKATAMS KELIAMI REIKALAVIMAI**

Kvalifikuotuose elektroninių spaudų sertifikatuose pateikiama:

- a) nuoroda (bent tokia forma, kad ją būtų galima tvarkyti automatizuotomis priemonėmis), kad sertifikatas išduotas kaip kvalifikuotas elektroninio spaudos sertifikatas;
  - b) duomenų rinkinys, kuriuo vienareikšmiškai nurodomas kvalifikuotas sertifikatus išduodantis kvalifikuotas patikimumo užtikrinimo paslaugų 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;
  - c) bent spaudos kūrėjo pavadinimas (vardas ir pavardė) ir, jei taikoma, oficialiame registre nurodytas registracijos numeris;
  - d) elektroninio spaudos patvirtinimo duomenys, atitinkantys elektroninio spaudos kūrimo duomenis;
  - e) duomenys apie sertifikato galiojimo laikotarpio pradžią ir pabaigą;
  - f) sertifikato identifikacinis kodas, kuris turi būti unikalus kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo atžvilgiu;
  - g) sertifikatą išduodančio kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo pažangusis elektroninis parašas arba pažangusis elektroninis spaudas;
  - h) vieta, kurioje galima nemokamai gauti sertifikatą, patvirtinantį g punkte nurodytą pažangųjį elektroninį parašą arba pažangųjį elektroninį spaudą;
  - i) paslaugų teikimo vieta, kurioje galima pasiteirauti dėl kvalifikuoto sertifikato galiojimo;
  - j) jeigu elektroninio spaudos kūrimo duomenys, susiję su elektroninio spaudos patvirtinimo duomenimis, yra kvalifikuotame elektroninio spaudos kūrimo įtaise, atitinkama tai nurodanti informacija pateikiama bent tokia forma, kad ją būtų galima tvarkyti automatizuotomis priemonėmis.
-

## IV PRIEDAS

**KVALIFIKUOTIEMS INTERNETO SVETAINĖS TAPATUMO NUSTATYMO SERTIFIKATAMS KELIAMI REIKALAVIMAI**

Kvalifikuotuose interneto svetainės tapatumo nustatymo sertifikatuose pateikiama:

- a) nuoroda (bent tokia forma, kad ją būtų galima tvarkyti automatizuotomis priemonėmis), kad sertifikatas išduotas kaip kvalifikuotas interneto svetainės tapatumo nustatymo sertifikatas;
  - b) duomenų rinkinys, kuriuo vienareikšmiškai nurodomas kvalifikuotus sertifikatus išduodantis kvalifikuotas patikimumo užtikrinimo paslaugų 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;
  - c) fizinio asmens atveju: bent to asmens, kuriam išduotas sertifikatas, vardas ir pavardė arba slapyvardis. Jei naudojamas slapyvardis, tai aiškiai nurodoma;
    - juridinio asmens atveju: bent juridinio asmens, kuriam išduotas sertifikatas, pavadinimas ir, jei taikoma, oficialiame registre nurodytas registracijos numeris;
  - d) fizinio ar juridinio asmens, kuriam išduotas sertifikatas, adreso duomenys, nurodant bent miestą ir valstybę, ir, jei taikoma, oficialiame registre nurodyti adreso duomenys;
  - e) domeno (-ų) vardas (-ai), kurį (-iuos) naudoja fizinis ar juridinis asmuo, kuriam išduotas sertifikatas;
  - f) duomenys apie sertifikato galiojimo laikotarpio pradžią ir pabaigą;
  - g) sertifikato identifikacinis kodas, kuris turi būti unikalus kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo atžvilgiu;
  - h) sertifikatą išduodančio kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo pažangusis elektroninis parašas arba pažangusis elektroninis spaudas;
  - i) vieta, kurioje galima nemokamai gauti sertifikatą, patvirtinantį h punkte nurodytą pažangųjį elektroninį parašą arba pažangųjį elektroninį spaudą;
  - j) sertifikato galiojimo statuso nustatymo paslaugų teikimo vieta, kurioje galima pasiteirauti dėl kvalifikuoto sertifikato galiojimo.
-