KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2015/1502

2015 m. rugsėjo 8 d.

kuriuo pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje 8 straipsnio 3 dalį nustatomos minimalios techninės specifikacijos ir procedūros dėl elektroninės atpažinties priemonių saugumo užtikrinimo lygių

(Tekstas svarbus EEE)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentą (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB ([1]), ypač į jo 8 straipsnio 3 dalį,

kadangi:

(1) Reglamento (ES) Nr. 910/2014 8 straipsnyje numatyta, kad elektroninės atpažinties schemoje, apie kurią pranešta pagal 9 straipsnio 1 dalį, turi būti apibrėžti elektroninės atpažinties priemonių, išduodamų pagal tą schemą, žemas, pakankamas ir (arba) aukštas saugumo užtikrinimo lygiai;

(2) būtina nustatyti minimalias technines specifikacijas, standartus ir procedūras, siekiant užtikrinti saugumo užtikrinimo lygių informacijos bendrą aiškinimą ir užtikrinti sąveikumą derinant elektroninės atpažinties schemų, apie kurias pranešta, nacionalinius saugumo užtikrinimo lygius su 8 straipsnyje numatytais saugumo užtikrinimo lygiais, kaip numatyta Reglamento (ES) Nr. 910/2014 12 straipsnio 4 dalies b punkte;

(3) nustatant šiame įgyvendinimo akte pateiktas specifikacijas ir procedūras buvo atsižvelgta į tarptautinį standartą ISO/IEC 29115 kaip į pagrindinį elektroninės atpažinties priemonių saugumo užtikrinimo lygiams taikomą tarptautinį standartą. Tačiau Reglamento (ES) Nr. 910/2014 turinys skiriasi nuo to tarptautinio standarto, visų pirma kiek tai susiję su tapatybės įrodymo ir tikrinimo reikalavimais, taip pat su tuo, kaip atsižvelgiama į valstybių narių tapatybės nustatymo tvarkos ir tapatybės nustatymo tvarkos esamose ES priemonėse skirtumus. Todėl nors priede ir remiamasi šiuo tarptautiniu standartu, jame neturėtų būti daroma nuoroda į jokį konkretų standarto ISO/IEC 29115 turinį;

(4) šis reglamentas parengtas remiantis rezultatais pagrįstu metodu, kuris laikomas tinkamiausiu – tai taip pat matyti iš apibrėžčių, vartojamų terminams ir sąvokoms apibrėžti. Juose atsižvelgiama į Reglamento (ES) Nr. 910/2014 tikslą, susijusį su elektroninės atpažinties priemonių saugumo užtikrinimo lygiais. Todėl nustatant šiame įgyvendinimo akte nustatytas specifikacijas ir procedūras turėtų būti kuo labiau atsižvelgiama į didelio masto bandomąjį projektą STORK, įskaitant pagal jį parengtas specifikacijas, ir į standarto ISO/IEC 29115 apibrėžtis ir sąvokas;

(5) priklausomai nuo aplinkybių, pagal kurias turi būti patikrintas tapatybės įrodymo aspektas, autoritetingų šaltinių forma gali būti įvairi, pavyzdžiui, be kita ko, registrai, dokumentai ar įstaigos. NET ir panašiomis aplinkybėmis autoritetingi šaltiniai skirtingose valstybėse narėse gali būti skirtingi;

(6) reikalavimuose dėl tapatybės įrodymo ir tikrinimo turėtų būti atsižvelgiama į skirtingas sistemas ir praktiką, kartu užtikrinant pakankamai aukštą saugumo lygį, būtiną reikiamam pasitikėjimui garantuoti. Todėl priimti procedūras, anksčiau naudotas kitu nei elektroninės atpažinties priemonių išdavimo tikslu, turėtų būti galima tik patvirtinus, kad šios procedūros atitinka reikalavimus, numatytus atitinkamam užtikrinimo lygiui;

([1]) OL L 257, 2014 8 28, p. 73.

(7) paprastai naudojami tam tikri tapatumo nustatymo veiksniai, tokie kaip bendros paslaptys, fiziniai įtaisai ir fizinės savybės. Vis dėlto siekiant padidinti tapatumo nustatymo proceso saugumą reikėtų skatinti naudoti daugiau tapatumo nustatymo veiksnių, ypač priklausančių įvairioms veiksnių kategorijoms;

(8) šiuo reglamentu neturėtų būti daromas poveikis juridinių asmenų atstovavimo teisėms. Vis dėlto priede turėtų būti numatyti reikalavimai dėl fizinių ir juridinių asmenų elektroninės atpažinties priemonių susiejimo;

(9) turėtų būti pripažįstama informacijos saugumo ir paslaugų valdymo sistemų svarba, taip pat pripažintos metodikos naudojimo bei principų, nustatytų standartuose, tokiuose kaip ISO/IEC 27000 ir EN ISO/IEC 20000 serijos, taikymo svarba;

(10) taip pat turėtų būti atsižvelgiama į gerąją praktiką, susijusią su saugumo užtikrinimo lygiais valstybėse narėse;

(11) tarptautiniais standartais grindžiamas IT saugumo sertifikavimas yra svarbi priemonė siekiant patikrinti, ar produktai atitinka šiame įgyvendinimo akte nustatytus saugumo reikalavimus;

(12) Reglamento (ES) Nr. 910/2014 48 straipsnyje nurodytas komitetas nepareiškė nuomonės per jo pirmininko nustatytą laikotarpį,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

1. Elektroninės atpažinties priemonių, išduotų pagal elektroninės atpažinties schemą, apie kurią pranešta, žemas, pakankamas ir aukštas saugumo užtikrinimo lygiai nustatomi remiantis priede pateiktomis specifikacijomis ir procedūromis.

2. Elektroninės atpažinties priemonių, išduotų pagal elektroninės atpažinties schemą, apie kurią pranešta, saugumo užtikrinimo lygiui apibrėžti naudojamos priede pateiktos specifikacijos ir procedūros, nustatant šių elementų patikimumą ir kokybę:

a) registracijos, kaip nustatyta šio reglamento priedo 2.1 skirsnyje pagal Reglamento (ES) Nr. 910/2014 8 straipsnio 3 dalies a punktą;

b) elektroninės atpažinties priemonių valdymo, kaip nustatyta šio reglamento priedo 2.2 skirsnyje pagal Reglamento (ES) Nr. 910/2014 8 straipsnio 3 dalies b ir f punktus;

c) tapatumo nustatymo, kaip nustatyta šio reglamento priedo 2.3 skirsnyje pagal Reglamento (ES) Nr. 910/2014 8 straipsnio 3 dalies c punktą;

d) valdymo ir organizavimo, kaip nustatyta šio reglamento priedo 2.4 skirsnyje pagal Reglamento (ES) Nr. 910/2014 8 straipsnio 3 dalies d ir e punktus.

3. Jeigu elektroninės atpažinties priemonė, išduota pagal elektroninės atpažinties schemą, apie kurią pranešta, atitinka aukštesnio saugumo užtikrinimo lygio reikalavimą, laikoma, kad ji atitinka lygiavertį žemesnio saugumo užtikrinimo lygio reikalavimą.

4. Jeigu atitinkamoje priedo dalyje nenurodyta kitaip, elektroninės atpažinties priemonė, išduota pagal elektroninės atpažinties schemą, apie kurią pranešta, turi atitikti visus priede išvardytus tam tikro saugumo užtikrinimo lygio elementus, kad atitiktų tą lygį.

2 straipsnis

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

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2015 m. rugsėjo 8 d.

Komisijos vardu
Pirmininkas
Jean-Claude JUNCKER

PRIEDAS

Techninės specifikacijos ir procedūros dėl elektroninės atpažinties priemonių, išduotų pagal elektroninės atpažinties schemą, apie kurią pranešta, žemo, pakankamo ir aukšto saugumo užtikrinimo lygių

1. **Terminų apibrėžtys**

Šiame priede vartojamų terminų apibrėžtys:

1) autoritetingas šaltinis – bet kokios formos šaltinis, kurio tikslūs duomenys, informacija ir (arba) įrodymai yra patikimi ir jus galima naudoti tapatybei įrodyti;

2) tapatumo nustatymo veiksnys – veiksnys, patvirtintas kaip esantis susijęs su asmeniu ir priklausantis prie vienos iš šių kategorijų:

   a) turėjimu grindžiamas tapatumo nustatymo veiksnys – tapatumo nustatymo veiksnys, kai subjektas turi įrodyti jį turįs;

   b) žiniomis grindžiamas tapatumo nustatymo veiksnys – tapatumo nustatymo veiksnys, kai subjektas turi įrodyti apie jį žinąs;

   c) būdingasis tapatumo nustatymo veiksnys – tapatumo nustatymo veiksnys, kuris grindžiamas fizinio asmens fizinėmis savybėmis ir subjektas turi įrodyti turįs tas fizines savybes;

3) dinaminis tapatumo nustatymas – elektroninis procesas, kuriuo naudojant kriptografijos ar kitus metodus suteikiama priemonė sukurti reikalaujamam elektroniniam įrodymui, kad subjektas kontroliuoja arba turi identifikavimo duomenis, ir kuris, priklausomai nuo subjekto ir subjekto tapatybę tikrinančios sistemos, kinta kiekvieną kartą nustatant tapatybę;

4) informacijos saugumo valdymo sistema – visuma procesų ir procedūrų, skirtų priimtinu lygiu valdyti rizikai, susijusiai su informacijos saugumu.

2. **Techninės specifikacijos ir procedūros**

Šiame priede nurodyti techninių specifikacijų ir procedūrų elementai naudotini siekiant nustatyti, kaip Reglamento (ES) Nr. 910/2014 8 straipsnyje pateikti reikalavimai ir kriterijai turi būti taikomi elektroninėms atpažinties priemonėms, išduotoms pagal elektroninės atpažinties schemą.

2.1. *Registracija*

2.1.1. Prašymo teikimas ir užregistravimas

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Užtikrinti, kad prašytojas būtų susipažinęs su elektroninės atpažinties priemonių naudojimo sąlygomis. 2. Užtikrinti, kad prašytojas būtų susipažinęs su rekomenduojamomis saugumo priemonėmis, susijusiomis su elektroninės atpažinties priemonėmis. 3. Rinkti reikiamus tapatybės duomenis, reikalingus tapatybei įrodyti ir patikrinti.
Pakankamas	Tokie patys, kaip žemo lygio.
Aukštas	Tokie patys, kaip žemo lygio.

2.1.2. Tapatybės įrodymas ir tikrinimas (fizinio asmens)

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Gali būti laikoma, kad asmuo turi įrodymų, kuriuos yra pripažinusi valstybė narė, kurioje teikiamas prašymas išduoti elektroninės atpažinties priemonę, ir kurie nurodo pareikštą tapatybę. 2. Gali būti laikoma, kad įrodymas yra tikras arba egzistuoja remiantis autoritetingu šaltiniu, ir atrodo, kad įrodymas yra galiojantis. 3. Autoritetingam šaltiniui žinoma, kad tvirtinama tapatybė egzistuoja, ir gali būti laikoma, kad asmuo, kuris pareiškia turintis tam tikrą tapatybę, yra tas pats.
Pakankamas	Be žemo lygio elementų, turi būti atitinkama viena iš 1–4 punktuose nurodytų sąlygų: 1. buvo patikrinta ir patvirtinta, kad asmuo turi įrodymų, pripažintų valstybės narės, kurioje teikiamas prašymas išduoti elektroninės atpažinties priemonę, ir kurie nurodo pareikštą tapatybę, ir įrodymai patikrinti siekiant nustatyti, ar jie yra tikri; arba, remiantis autoritetingu šaltiniu, žinoma, kad jie egzistuoja ir yra susiję su realiu asmeniu, ir buvo imtasi veiksmų siekiant sumažinti riziką, kad asmens tapatybė nėra tvirtinama tapatybė, atsižvelgiant, pavyzdžiui, į riziką, kad įrodymai gali būti prarasti, pavogti, jų galiojimas sustabdytas, panaikinti arba pasibaigusio galiojimo; arba 2. asmens tapatybės dokumentas pateiktas per registracijos procesą jo išdavimo valstybėje narėje ir atrodo, kad dokumentas yra susijęs su jį pateikusiu asmeniu, ir buvo imtasi veiksmų siekiant sumažinti riziką, kad asmens tapatybė nėra pareikšta tapatybė, atsižvelgiant, pavyzdžiui, į riziką, kad dokumentai gali būti prarasti, pavogti, jų galiojimas sustabdytas, panaikinti arba pasibaigusio galiojimo; arba 3. jeigu anksčiau toje pačioje valstybėje narėje viešojo arba privačiojo subjekto naudotomis procedūromis siekiant kito tikslo nei išduoti elektroninės atpažinties priemonę, numatomas 2.1.2 skirsnyje nustatytam pakankamo lygio saugumo užtikrinimui lygiavertis saugumo užtikrinimas, įstaigai, atsakingai už registraciją, nereikia kartoti šių ankstesnių procedūrų, jeigu šį lygiavertį saugumo užtikrinimą patvirtino Europos Parlamento ir Tarybos reglamento (EB) Nr. 765/2008 [1] 2 straipsnio 13 dalyje nurodyta atitikties vertinimo įstaiga, arba lygiavertė įstaiga; arba 4. jeigu elektroninės atpažinties priemonės išduotos remiantis galiojančiomis pakankamo arba aukšto saugumo užtikrinimo lygio elektroninės atpažinties priemonėmis, apie kurias pranešta, ir atsižvelgiant į asmens tapatybės duomenų pakeitimo riziką, nėra būtina kartoti tapatybės įrodymo ir tikrinimo procesų; jeigu apie elektronines atpažinties priemones, kuriomis yra remiamasi, nebuvo pranešta, pakankamą arba aukštą saugumo užtikrinimo lygį turi patvirtinti atitikties vertinimo įstaiga, nurodyta Reglamento (EB) Nr. 765/2008 2 straipsnio 13 dalyje, arba lygiavertė įstaiga.

Saugumo užtikrinimo lygis	Būtini elementai
Aukštas	Turi būti laikomasi 1 arba 2 punkto reikalavimų: 1. Be pakankamo lygio elementų, turi būti atitinkama viena iš a–c punktuose nurodytų sąlygų: a) jeigu buvo patikrinta ir patvirtinta, kad asmuo turi fotografinių arba biometrinių atpažinties įrodymų, pripažintų valstybės narės, kurioje teikiamas prašymas išduoti elektroninės atpažinties priemonę, ir tie įrodymai nurodo pareikštą tapatybę, tie įrodymai tikrinami siekiant nustatyti, ar jie galioja, remiantis autoritetingu šaltiniu, ir prašytojo tapatybė nustatoma kaip tvirtinama tapatybė, lyginant vieną ar kelias asmens fizines savybes su autoritetingu šaltiniu, arba b) jeigu anksčiau toje pačioje valstybėje narėje viešojo arba privačiojo subjekto naudotomis procedūromis siekiant kito tikslo nei išduoti elektroninės atpažinties priemonę, numatomas 2.1.2 skirsnyje nustatytam aukšto saugumo užtikrinimo lygio saugumo užtikrinimui lygiavertis saugumo užtikrinimas, įstaigai, atsakingai už registraciją, nereikia kartoti šių ankstesnių procedūrų, jeigu šį lygiavertį saugumo užtikrinimą patvirtino Reglamento (EB) Nr. 765/2008 2 straipsnio 13 dalyje nurodyta atitikties vertinimo įstaiga arba lygiavertė įstaiga, ir imtasi veiksmų siekiant įrodyti, kad šių ankstesnių procedūrų rezultatai tebegalioja; arba c) jeigu elektroninės atpažinties priemonės išduotos remiantis galiojančiomis aukšto saugumo užtikrinimo lygio elektroninės atpažinties priemonėmis, apie kurias pranešta, ir atsižvelgiant į asmens tapatybės duomenų pakeitimo riziką, nėra būtina kartoti tapatybės įrodymo ir tikrinimo procesų. Jeigu apie elektronines atpažinties priemones, kuriomis yra remiamasi, nebuvo pranešta, aukštą saugumo užtikrinimo lygį turi patvirtinti atitikties vertinimo įstaiga, nurodyta Reglamento (EB) Nr. 765/2008 2 straipsnio 13 dalyje, arba lygiavertė įstaiga, ir imtasi veiksmų, siekiant įrodyti, kad elektroninių atpažinties priemonių, apie kurias pranešta, ankstesnės išdavimo procedūros rezultatai tebegalioja. ARBA 2. Jeigu prašytojas nepateikia jokių pripažintų fotografinių ar biometrinių tapatybės atpažinties įrodymų, taikomos tos pačios procedūros, kurios nacionaliniu lygiu naudojamos įstaigos, atsakingos už registraciją, valstybėje narėje, siekiant gauti tokius pripažintus fotografinius arba biometrinius tapatybės nustatymo įrodymus.

([1]) 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 panaikinantis Reglamentą (EEB) Nr. 339/93 (OL L 218, 2008 8 13, p. 30).

2.1.3. Tapatybės įrodymas ir tikrinimas (juridinio asmens)

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Juridinio asmens tvirtinama tapatybė įrodoma remiantis valstybės narės, kurioje teikiamas prašymas išduoti elektroninės atpažinties priemones, pripažintais įrodymais.

Saugumo užtikrinimo lygis	Būtini elementai
	2. Atrodo, kad įrodymai yra galiojantys, ir gali būti laikoma, kad jie yra tikri arba egzistuoja, remiantis autoritetingu šaltiniu, jeigu juridinio asmens įtraukimas į autoritetingą šaltinį yra savanoriškas ir reglamentuojamas juridinio asmens ir autoritetingo šaltinio susitarimu. 3. Autoritetingam šaltiniui nežinoma, ar juridinis asmuo yra būklėje, kuri neleistų jam veikti kaip tam juridiniam asmeniui.
Pakankamas	Be žemo lygio elementų, turi būti atitinkama viena iš 1–3 punktuose nurodytų sąlygų: 1. juridinio asmens pareikšta tapatybė įrodoma remiantis valstybės narės, kurioje pateiktas prašymas išduoti elektroninės atpažinties priemones, pripažintais įrodymais, be kita ko, juridinio asmens pavadinimu, teisine forma ir (jei taikoma) registracijos numeriu ir įrodymai tikrinami siekiant nustatyti, ar jie tikri, arba žinoma, kad jie egzistuoja, remiantis autoritetingu šaltiniu, jeigu juridinio asmens įtraukimas į autoritetingą šaltinį yra reikalingas tam, kad juridinis asmuo galėtų veikti savo sektoriuje, ir buvo imtasi veiksmų siekiant sumažinti riziką, kad juridinio asmens tapatybė nėra pareikšta tapatybė, atsižvelgiant, pavyzdžiui, į riziką, kad dokumentai gali būti prarasti, pavogti, jų galiojimas sustabdytas, panaikinti arba pasibaigusio galiojimo; arba 2. jeigu anksčiau toje pačioje valstybėje narėje viešojo arba privačiojo subjekto naudotomis procedūromis siekiant kito tikslo nei išduoti elektroninės atpažinties priemonę, numatomas 2.1.3 skirsnyje nustatytam pakankamo lygio saugumo užtikrinimui lygiavertis saugumo užtikrinimas, įstaigai, atsakingai už registraciją, nereikia kartoti šių ankstesnių procedūrų, jeigu šį lygiavertį saugumo užtikrinimą patvirtino Reglamento (EB) Nr. 765/2008 2 straipsnio 13 dalyje nurodyta atitikties vertinimo įstaiga, arba lygiavertė įstaiga; arba 3. jeigu elektroninės atpažinties priemonės išduotos remiantis galiojančiomis pakankamo arba aukšto saugumo užtikrinimo lygio elektroninės atpažinties priemonėmis, apie kurias pranešta, nėra būtina kartoti tapatybės įrodymo ir tikrinimo procesų. jeigu apie elektroninės atpažinties priemones, kuriomis yra remiamasi, nebuvo pranešta, pakankamą arba aukštą saugumo užtikrinimo lygį turi patvirtinti atitikties vertinimo įstaiga, nurodyta Reglamento (EB) Nr. 765/2008 2 straipsnio 13 dalyje, arba lygiavertė įstaiga.
Aukštas	Be pakankamo lygio elementų, turi būti atitinkama viena iš 1–3 punktuose nurodytų sąlygų: 1. juridinio asmens tvirtinama tapatybė įrodoma remiantis valstybės narės, kurioje pateiktas prašymas išduoti elektroninės atpažinties priemones, pripažintais įrodymais, be kita ko, juridinio asmens pavadinimu, teisine forma ir bent vienu nacionalinėje aplinkoje naudojamu unikaliu identifikatoriumi, susijusiu su juridiniu asmeniu, ir įrodymai tikrinami siekiant nustatyti, ar jie yra tikri, remiantis autoritetingu šaltiniu; arba

Saugumo užtikrinimo lygis	Būtini elementai
	2. jeigu anksčiau toje pačioje valstybėje narėje viešojo arba privačiojo subjekto naudotomis procedūromis siekiant kito tikslo, nei išduoti elektroninės atpažinties priemonę, numatomas 2.1.3 skirsnyje nustatytam aukšto lygio saugumo užtikrinimui lygiavertis saugumo užtikrinimas, įstaigai, atsakingai už registraciją, nereikia kartoti šių ankstesnių procedūrų, jeigu šį lygiavertį saugumo užtikrinimą patvirtino Reglamento (EB) Nr. 765/2008 2 straipsnio 13 dalyje nurodyta atitikties vertinimo įstaiga arba lygiavertė įstaiga, ir imtasi veiksmų siekiant įrodyti, kad šių ankstesnių procedūrų rezultatai tebegalioja; arba 3. jeigu elektroninės atpažinties priemonės išduotos remiantis galiojančiomis aukšto saugumo užtikrinimo lygio elektroninės atpažinties priemonėmis, apie kurias pranešta, nėra būtina kartoti tapatybės įrodymo ir tikrinimo procesų. Jeigu apie elektronines atpažinties priemones, kuriomis yra remiamasi, nebuvo pranešta, aukštą saugumo užtikrinimo lygį turi patvirtinti atitikties vertinimo įstaiga, nurodyta Reglamento (EB) Nr. 765/2008 2 straipsnio 13 dalyje, arba lygiavertė įstaiga, ir imtasi veiksmų, siekiant įrodyti, kad elektroninių atpažinties priemonių, apie kurias pranešta, ankstesnės išdavimo procedūros rezultatai tebegalioja.

2.1.4. Fizinių ir juridinių asmenų elektroninės atpažinties priemonių susiejimas

Atitinkamais atvejais fizinio asmens elektroninės atpažinties priemonių ir juridinio asmens elektroninės atpažinties priemonių susiejimui (toliau – susiejimas) taikomos šios sąlygos:

1) turi būti įmanoma sustabdyti ir (arba) atšaukti susiejimą. Susiejimo gyvavimo ciklas (pvz., aktyvavimas, sustabdymas, atnaujinimas, atšaukimas) tvarkomas laikantis nacionaliniu lygiu pripažintų procedūrų.

2) Fizinis asmuo, kurio elektroninės atpažinties priemonės yra susietos su juridinio asmens elektroninės atpažinties priemonėmis, pagal nacionaliniu lygiu pripažintas procedūras susiejimą gali įgalioti kitam fiziniam asmeniui. Vis dėlto atsakomybė išlieka įgaliojančiojo fizinio asmens.

3) Susiejimas atliekamas taip:

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Patikrinta, kad juridinio asmens vardu veikiančio fizinio asmens tapatybės įrodymo patikrinimas atliktas žemu arba aukštesniu lygiu. 2. Susiejimas nustatytas remiantis nacionaliniu lygiu pripažintomis procedūromis. 3. Autoritetingam šaltiniui nežinoma, kad fizinis asmuo yra būklėje, dėl kurios jis negalėtų veikti juridinio asmens vardu.
Pakankamas	Žemo lygio 3 punkto, be to: 1. Patikrinta, kad juridinio asmens vardu veikiančio fizinio asmens tapatybės įrodymo patikrinimas atliktas pakankamu arba aukštu lygiu.

Saugumo užtikrinimo lygis	Būtini elementai
	2. Susiejimas nustatytas remiantis nacionaliniu lygiu pripažintomis procedūromis, kurį atlikus susiejimas įregistruotas autoritetingame šaltinyje. 3. Susiejimas buvo patikrintas remiantis autoritetingo šaltinio informacija.
Aukštas	Žemo lygio 3 punkto ir pakankamo lygio 2 punkto, be to: 1. Patikrinta, kad juridinio asmens vardu veikiančio fizinio asmens tapatybės įrodymo patikrinimas atliktas aukštu lygiu. 2. Susiejimas patikrintas remiantis nacionalinėje aplinkoje naudojamu unikaliu identifikatoriumi, susijusiu su juridiniu asmeniu, taip pat remiantis autoritetingo šaltinio informacija, kuria nurodomas konkretus fizinis asmuo.

2.2. *Elektroninės atpažinties priemonių valdymas*

2.2.1. Elektroninės atpažinties priemonių savybės ir struktūra

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Elektroninės atpažinties priemonėje naudojamas bent vienas tapatumo nustatymo veiksnys. 2. Elektroninės atpažinties priemonė sukurta taip, kad išdavėjas imtųsi pagrįstų veiksmų patikrinti, kad tik asmuo, kuriam ji priklauso, galėtų ją kontroliuoti arba turėti.
Pakankamas	1. Elektroninės atpažinties priemonėje naudojami bent du skirtingų kategorijų tapatumo nustatymo veiksniai. 2. Elektroninės atpažinties priemonė sukurta taip, kad galima būtų laikyti, kad ją gali naudoti tik asmuo, kuriam ji priklauso, ir kuris ją kontroliuoja arba turi.
Aukštas	Pakankamo lygio, be to: 1. Elektroninės atpažinties priemonė apsaugo nuo kopijavimo ir klastojimo, taip pat nuo išpuolių vykdytojų su dideliu išpuolių vykdymo potencialu. 2. Elektroninės atpažinties priemonė sukurta taip, kad asmuo, kuriam ji priklauso, ją galėtų patikimai apsaugoti nuo kitų asmenų naudojimo.

2.2.2. Išdavimas, pristatymas ir aktyvavimas

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	Išduota elektroninės atpažinties priemonė pristatoma naudojant mechanizmą, kuriuo galima laikyti, kad ji pasiekė tik tą asmenį, kuriam ji numatyta.
Pakankamas	Išduota elektroninės atpažinties priemonė pristatoma naudojant mechanizmą, kuriuo galima laikyti, kad ji pristatyta tik tam asmeniui, kuriam ji priklauso.
Aukštas	Aktyvavimo procesu patvirtinama, kad elektroninės atpažinties priemonė buvo pristatyta tik tam asmeniui, kuriam ji priklauso.

2.2.3. Sustabdymas, atšaukimas ir pakartotinis aktyvavimas

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Elektroninės atpažinties priemonių galiojimą galima laiku ir veiksmingai sustabdyti ir (arba) jas atšaukti. 2. Imtasi priemonių siekiant užkirsti kelią neteisėtam galiojimo sustabdymui, atšaukimui ir (arba) pakartotinam aktyvavimui. 3. Pakartotinis aktyvavimas galimas tik jeigu toliau atitinkami tie patys iki galiojimo sustabdymo arba atšaukimo nustatyti patikimumo užtikrinimo reikalavimai.
Pakankamas	Tokie patys, kaip žemo lygio.
Aukštas	Tokie patys, kaip žemo lygio.

2.2.4. Atnaujinimas ir pakeitimas

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	Atsižvelgiant į asmens tapatybės duomenų pakeitimo riziką, atnaujinimui arba pakeitimui turi būti keliami tokie patys saugumo užtikrinimo reikalavimai kaip pradiniam tapatybės įrodymo nustatymui ir tikrinimui, arba atnaujinimas ar pakeitimas turi būti pagrįstas tokio paties arba aukštesnio patikimumo lygio galiojančiomis elektroninės atpažinties priemonėmis.
Pakankamas	Tokie patys, kaip žemo lygio.
Aukštas	Žemo lygio, be to: kai atnaujinimas ar pakeitimas pagrįstas galiojančiomis elektroninės atpažinties priemonėmis, tapatybės duomenys tikrinami su autoritetingu šaltiniu.

2.3. *Tapatumo nustatymas*

Šiame skirsnyje daugiausia dėmesio skiriama grėsmėms, susijusioms su tapatumo nustatymo mechanizmu, ir išvardijami kiekvieno saugumo užtikrinimo lygio reikalavimai. Šiame skirsnyje laikoma, kad kontrolės priemonės atitinka tam tikro lygio riziką.

2.3.1. Tapatumo nustatymo mechanizmas

Šioje lentelėje pateikti tapatumo nustatymo mechanizmo, pagal kurį fizinis arba juridinis asmuo naudojasi elektroninės atpažinties priemone, kad patvirtintų savo tapatybę pasikliaujančiajai šaliai, kiekvieno saugumo užtikrinimo lygio reikalavimai.

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Prieš pateikiant asmens tapatybės duomenis patikimai tikrinama elektroninės atpažinties priemonė ir jos galiojimas. 2. Jeigu pagal tapatumo nustatymo mechanizmą turi būti saugomi asmens tapatybės duomenys, ta informacija apsaugoma, siekiant ją apsaugoti nuo praradimo ir pažeidimo, įskaitant analizavimą neprisijungus prie interneto. 3. Tapatumo nustatymo mechanizmu įgyvendinamos tokios saugumo kontrolės priemonės elektroninės atpažinties priemonėms patikrinti, kad išpuolių vykdytojas su baziniu sustiprintu išpuolių vykdymo potencialu, bandydamas atspėti, pasiklausyti, keisti ir pakartotinai išklausyti pranešimą, vargiai galėtų apeiti tapatumo nustatymo mechanizmus.

Saugumo užtikrinimo lygis	Būtini elementai
Pakankamas	Žemo lygio, be to: 1. prieš pateikiant asmens tapatybės duomenis, vykdant dinaminį tapatumo nustatymą patikimai tikrinama elektroninės atpažinties priemonė ir jos galiojimas. 2. Tapatumo nustatymo mechanizmu įgyvendinamos tokios saugumo kontrolės priemonės elektroninės atpažinties priemonėms patikrinti, kad išpuolių vykdytojas su vidutiniu išpuolių vykdymo potencialu, bandydamas atspėti, pasiklausyti, keisti ir pakartotinai išklausyti pranešimą, vargiai galėtų apeiti tapatumo nustatymo mechanizmus.
Aukštas	Pakankamo lygio, be to: tapatumo nustatymo mechanizmu įgyvendinamos tokios saugumo kontrolės priemonės elektroninės atpažinties priemonėms patikrinti, kad išpuolių vykdytojas su dideliu išpuolių vykdymo potencialu, bandydamas atspėti, pasiklausyti, keisti ir pakartotinai išklausyti pranešimą, vargiai galėtų apeiti tapatumo nustatymo mechanizmus.

2.4. *Valdymas ir organizavimas*

Visi dalyviai, teikiantys paslaugą, susijusią su tarpvalstybinio lygmens elektronine atpažintimi (toliau – teikėjai), turi būti nustatę dokumentais patvirtintą informacijos saugumo valdymo praktiką, politikos priemones, rizikos valdymo metodus ir kitas pripažintas kontrolės priemones, kad atitinkamų valstybių narių elektroninės atpažinties schemų valdymo organams galėtų garantuoti, jog įdiegta veiksminga praktika. 2.4 skirsnyje laikoma, kad visi reikalavimai/elementai atitinka tam tikro lygio riziką.

2.4.1. Bendrosios nuostatos

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Paslaugų teikėjai, teikiantys bet kokią paslaugą, kuriai taikomas šis reglamentas, yra valdžios institucija ar juridinis subjektas, tokiu pripažįstamas pagal valstybės narės nacionalinę teisę; jie turi nustatytą struktūrą ir visapusiškai veikia visose su paslaugų teikimu susijusiose srityse. 2. Paslaugų teikėjai laikosi visų jiems tenkančių teisinių reikalavimų, susijusių su paslaugos valdymu ir teikimu, įskaitant reikalavimus, susijusius su informacija, kurios gali būti prašoma, tapatybės įrodymo nustatymu, su tuo, kokia informacija gali būti saugoma ir kiek laiko. 3. Paslaugų teikėjai gali įrodyti savo gebėjimą prisiimti atsakomybės už žalą riziką, taip pat turėt pakankamų finansinių išteklių tęsti veiklą ir teikti paslaugas. 4. Paslaugų teikėjai yra atsakingi už bet kokių kitam subjektui perduotų savo įsipareigojimų vykdymą ir turi laikytis schemos politikos nuostatų taip, tarsi tas pareigas būtų įvykdę patys paslaugų teikėjai. 5. Elektroninės atpažinties schemose, kurios nesukurtos pagal nacionalinę teisę, turi būti numatytas veiksmingas nutraukimo planas. Tokiame plane turi būti numatyta, kokia tvarka nutraukti paslaugą arba jos tęsimą paskirti kitam paslaugų teikėjui, kaip atitinkamos valdžios institucijos ir galutiniai naudotojai turi būti informuojami ir kaip pagal schemos politiką įrašai turi būti saugomi, laikomi ir sunaikinami.
Pakankamas	Tokie patys, kaip žemo lygio.
Aukštas	Tokie patys, kaip žemo lygio.

2.4.2. Paskelbti pranešimai ir informacija naudotojams

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Paskelbta paslaugos apibrėžtis, kurioje pateikti visi taikomi terminai, sąlygos ir mokesčiai, įskaitant bet kokius naudojimosi ja apribojimus. Paslaugos apibrėžtyje turi būti nustatytos privatumo taisyklės. 2. Turi būti nustatytos tinkamos politikos nuostatos ir procedūros siekiant užtikrinti, kad paslaugos naudotojams būtų laiku ir patikimu būdu pranešta apie bet kokius paslaugos apibrėžties ir taikomų terminų, sąlygų ir privatumo taisyklių pasikeitimus. 3. Turi būti nustatytos tinkamos politikos nuostatos ir procedūros, pagal kurias būtų visapusiškai ir deramai atsakoma į prašymus pateikti informacijos.
Pakankamas	Tokie patys, kaip žemo lygio.
Aukštas	Tokie patys, kaip žemo lygio.

2.4.3. Informacijos saugumo valdymas

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	Veikia veiksminga informacijos saugumo valdymo sistema, skirta informacijos saugumo rizikai valdyti ir kontroliuoti.
Pakankamas	Žemo lygio, be to: informacijos saugumo valdymo sistemoje laikomasi pasiteisinusių standartų arba principų, skirtų informacijos saugumo rizikai valdyti ir kontroliuoti.
Aukštas	Tokie patys, kaip pakankamo lygio.

2.4.4. Įrašų saugojimas

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Registruoti ir išlaikyti atitinkamą informaciją naudojant veiksmingą įrašų valdymo sistemą, atsižvelgiant į taikomus teisės aktus ir gerąją praktiką, susijusius su duomenų apsauga ir saugojimu. 2. Laikyti informaciją, kiek tai leidžiama pagal nacionalinę teisę arba kitą nacionalinę administracinę tvarką, ir apsaugoti bei išsaugoti duomenis tiek, kiek būtina siekiant atlikti auditą ir saugumo pažeidimų tyrimus; po to duomenys turi būti saugiai sunaikinti.
Pakankamas	Tokie patys, kaip žemo lygio.
Aukštas	Tokie patys, kaip žemo lygio.

2.4.5. Įrenginiai ir darbuotojai

Šioje lentelėje pateikiami reikalavimai įrenginiams, darbuotojams ir (jei taikytina) subrangovams, kurie vykdo pareigas pagal šį reglamentą. Atitiktis kiekvienam reikalavimui turi būti proporcinga rizikos laipsniui, susijusiam su nustatytu saugumo užtikrinimo lygiu.

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Įdiegtos procedūros, kuriomis užtikrinama, kad darbuotojai ir subrangovai būtų pakankamai išmokyti, būtų kvalifikuoti ir turėtų patirties, reikalingos vykdant atitinkamas funkcijas. 2. Yra pakankamai darbuotojų ir subrangovų, galinčių tinkamai vykdyti paslaugą ir suteikti išteklių pagal jos politiką ir procedūras. 3. Įrenginiai, naudojami teikiant paslaugą, yra nuolat stebimi ir apsaugo nuo aplinkos įvykių daromos žalos, neleistinos prieigos ir kitų veiksnių, kurie gali paveikti paslaugos saugumą. 4. Įrenginiai, naudojami teikiant paslaugą, užtikrina, kad patekti į zonas, kuriose laikoma arba tvarkoma asmens, kriptografinė ar kita neskelbtina informacija, galėtų tik įgalioti darbuotojai ar subrangovai.
Pakankamas	Tokie patys, kaip žemo lygio.
Aukštas	Tokie patys, kaip žemo lygio.

2.4.6. Techninė kontrolė

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	1. Veikia proporcingos techninės kontrolės priemonės, skirtos paslaugų saugumui kylančiai rizikai valdyti ir tvarkomos informacijos konfidencialumui, vientisumui ir prieinamumui apsaugoti. 2. Elektroninių ryšių kanalai, naudojami keistis asmens arba neskelbtina informacija, yra apsaugoti nuo pasiklausymo, keitimo ir pakartotino išklausymo. 3. Prieiga prie neskelbtinos kriptografinės medžiagos, jeigu ji naudojama elektroninės atpažinties priemonėms išduoti ir tapatumui nustatyti, suteikiama tik toms funkcijoms ir taikomosioms programoms, kurioms prieiga yra būtina. Turi būti užtikrinta, kad tokia medžiaga niekada nebūtų nuolat saugoma paprasto teksto pavidalu. 4. Veikia procedūros, kuriomis užtikrinama, kad saugumas būtų nuolat išlaikytas ir kad būtų sugebama reaguoti į rizikos lygių pokyčius, incidentus ir saugumo pažeidimus. 5. Visos laikmenos, kuriose laikoma asmens, kriptografinė ar kita neskelbtina informacija, saugomos, transportuojamos ir šalinamos saugiai ir patikimai.
Pakankamas	Tokie patys, kaip žemo lygio, be to: neskelbtina kriptografinė medžiaga, jeigu ji naudojama elektroninės atpažinties priemonėms išduoti ir tapatumui nustatyti, yra apsaugota nuo klastojimo.
Aukštas	Tokie patys, kaip pakankamo lygio.

2.4.7. Atitiktis ir auditas

Saugumo užtikrinimo lygis	Būtini elementai
Žemas	Periodiškai vykdomas vidaus auditas, apimantis visas su teikiamomis paslaugomis susijusias sritis, siekiant užtikrinti, kad būtų laikomasi atitinkamų politikos nuostatų.

Saugumo užtikrinimo lygis	Būtini elementai
Pakankamas	Periodiškai vykdomas nepriklausomas vidaus arba išorės auditas, apimantis visas su teikiamomis paslaugomis susijusias sritis, siekiant užtikrinti, kad būtų laikomasi atitinkamų politikos nuostatų.
Aukštas	1. Periodiškai vykdomas nepriklausomas išorės auditas, apimantis visas su teikiamomis paslaugomis susijusias sritis, siekiant užtikrinti, kad būtų laikomasi atitinkamų politikos nuostatų. 2. Tais atvejais, kai schemą tiesiogiai valdo valdžios institucija, ji tikrinama pagal nacionalinę teisę.