Europos Sąjungos
oficialusis leidinys

L 194

Leidimas
lietuvių kalba

Teisės aktai

59 tomas

2016 m. liepos 19 d.

Turinys

LT

Aktai, kurių pavadinimai spausdinami paprastu šriftu, yra susiję su kasdieniu žemės ūkio reikalų valdymu ir paprastai galioja ribotą laikotarpį.

Visų kitų aktų pavadinimai spausdinami ryškesniu šriftu ir prieš juos dedama žvaigždutė.

I

(Teisėkūros procedūra priimami aktai)

DIREKTYVOS

EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA (ES) 2016/1148

2016 m. liepos 6 d.

dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti

EUROPOS PARLAMENTAS IR EUROPOS SĄJUNGOS TARYBA,

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

atsižvelgdami į Europos Komisijos pasiūlymą,

teisėkūros procedūra priimamo akto projektą perdavus nacionaliniams parlamentams,

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

laikydamiesi įprastos teisėkūros procedūros ([2]),

kadangi:

(1) tinklų ir informacinėms sistemoms bei paslaugoms tenka gyvybiškai svarbus vaidmuo visuomenėje. Jų patikimumas ir saugumas yra labai svarbūs ekonominei ir visuomeninei veiklai, ypač vidaus rinkos veikimui;

(2) saugumo incidentų mastas, dažnumas ir poveikis didėja ir kelia didelę grėsmę tinklų ir informacinių sistemų veikimui. Tos sistemos taip pat gali tapti tyčinių žalingų veiksmų, kuriais siekiama padaryti žalą sistemų veikimui arba jį sutrikdyti, taikiniu. Tokie incidentai gali trukdyti vykdyti ekonominę veiklą, sukelti didelių finansinių nuostolių, pakirsti naudotojų pasitikėjimą ir padaryti didelę žalą Sąjungos ekonomikai;

(3) tinklų ir informacinėms sistemoms, visų pirma internetui, tenka esminis vaidmuo palengvinant tarpvalstybinį prekių, paslaugų ir asmenų judėjimą. Dėl tokio tarpvalstybinio pobūdžio didelis tų sistemų veikimo tyčinis ar netyčinis sutrikdymas, nepriklausomai nuo jo vietos, gali paveikti atskiras valstybes nares ir visą Sąjungą. Todėl tinklų ir informacinių sistemų saugumas yra būtinas, kad vidaus rinka veiktų sklandžiai;

(4) pasinaudojant reikšminga pažanga, padaryta valstybių narių Europos forume skatinant diskusijas ir keitimąsi gerąja politikos patirtimi, įskaitant Europos bendradarbiavimo kibernetinių krizių atveju principų parengimą, turėtų būti įsteigta Bendradarbiavimo grupė, sudaryta iš valstybių narių, Komisijos bei Europos Sąjungos tinklų ir

([1]) OL C 271, 2013 9 19, p. 133.
([2]) 2014 m. kovo 13 d. Europos Parlamento pozicija (dar nepaskelbta Oficialiajame leidinyje) ir 2016 m. gegužės 17 d. Tarybos per pirmąjį svarstymą priimta pozicija (dar nepaskelbta Oficialiajame leidinyje). 2016 m. liepos 6 d. Europos Parlamento pozicija (dar nepaskelbta Oficialiajame leidinyje).

informacijos apsaugos agentūros (ENISA) atstovų, kuri remtų ir palengvintų strateginį valstybių narių bendradarbiavimą tinklų ir informacinių sistemų saugumo srityje. Kad tos grupės veikla būtų veiksminga ir įtrauki, itin svarbu, kad visos valstybės narės turėtų būtiniausių pajėgumų ir strategiją, užtikrinančią aukštą tinklų ir informacinių sistemų saugumo lygį savo teritorijoje. Be to, saugumo ir pranešimų reikalavimai turėtų būti taikomi esminių paslaugų operatoriams ir skaitmeninių paslaugų teikėjams siekiant skatinti rizikos valdymo kultūrą ir užtikrinti, kad būtų pranešama apie didžiausius incidentus;

(5) esamų pajėgumų nepakanka, kad būtų galima užtikrinti aukštą tinklų ir informacinių sistemų saugumo lygį Sąjungoje. Valstybių narių parengties lygis yra labai skirtingas, todėl visoje Sąjungoje susiformavo skirtingi požiūriai. Dėl to vartotojų ir įmonių apsaugos lygis yra nevienodas, o tai kenkia bendram tinklų ir informacinių sistemų saugumo lygiui Sąjungoje. Dėl to, kad nėra nustatyta bendrų reikalavimų esminių paslaugų operatoriams ir savo ruožtu skaitmeninių paslaugų teikėjams, neįmanoma sukurti bendradarbiavimo Sąjungos lygmeniu visuotinio veiksmingo mechanizmo. Universitetams ir mokslinių tyrimų centrams tenka lemiamas vaidmuo skatinant tų sričių mokslinius tyrimus, technologinę plėtrą ir inovacijas;

(6) todėl norint veiksmingai spręsti tinklų ir informacinių sistemų saugumo problemas, reikia visuotinio požiūrio Sąjungos lygmeniu, apimančio bendrus būtiniausius gebėjimų stiprinimo ir planavimo reikalavimus, keitimąsi informacija, bendradarbiavimo ir bendrus saugumo reikalavimus esminių paslaugų operatoriams ir skaitmeninių paslaugų teikėjams. Vis dėlto esminių paslaugų operatoriams ir skaitmeninių paslaugų teikėjams nedraudžiama įgyvendinti griežtesnes saugumo priemones nei tos, kurios numatytos pagal šią direktyvą;

(7) siekiant aprėpti visus atitinkamus incidentus ir rizikos rūšis, ši direktyva turėtų būti taikoma tiek esminių paslaugų operatoriams, tiek skaitmeninių paslaugų teikėjams. Vis dėlto nustatytos esminių paslaugų operatorių ir skaitmeninių paslaugų teikėjų pareigos neturėtų būti taikomos įmonėms, teikiančioms viešųjų ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugas, kaip apibrėžta Europos Parlamento ir Tarybos direktyvoje 2002/21/EB ([1]), kurioms taikomi konkretūs saugumo ir vientisumo reikalavimai, nustatyti toje direktyvoje, ir tos pareigos neturėtų būti taikomos patikimumo užtikrinimo paslaugų teikėjams, kaip apibrėžta Europos Parlamento ir Tarybos reglamente (ES) Nr. 910/2014 ([2]), kuriems taikomi tame reglamente nustatyti saugumo reikalavimai;

(8) šia direktyva neturėtų būti daromas poveikis kiekvienos valstybės narės galimybei imtis priemonių, būtinų gyvybiniams jos saugumo interesams užtikrinti, viešajai tvarkai palaikyti bei visuomenės saugumui užtikrinti, ir sudaryti sąlygas tirti bei išsiaiškinti nusikalstamas veikas ir už jas patraukti baudžiamojon atsakomybėn. Pagal Sutarties dėl Europos Sąjungos veikimo (toliau – SESV) 346 straipsnį jokia valstybė narė neprivalo teikti informacijos, kurios atskleidimą ji laiko prieštaraujančiu gyvybiniams savo saugumo interesams. Šiomis aplinkybėmis svarbus Tarybos sprendimas 2013/488/ES ([3]) ir informacijos neatskleidimo susitarimai ar neoficialūs informacijos neatskleidimo susitarimai, pavyzdžiui, Srauto kontrolės protokolas;

(9) tam tikri ekonomikos sektoriai jau yra arba ateityje gali būti reglamentuojami konkretiems sektoriams taikomais Sąjungos teisės aktais, į kuriuos įtrauktos taisyklės, susijusios su tinklų ir informacinių sistemų saugumu. Kai į tuos Sąjungos teisės aktus yra įtrauktos nuostatos, kuriomis nustatomi reikalavimai dėl tinklų ar informacinių sistemų saugumo arba pranešimų apie incidentus, tos nuostatos turėtų būti taikomos, jei jose nustatyti reikalavimai, kurių poveikis yra bent lygiavertis šioje direktyvoje nustatytų pareigų poveikiui. Tokiu atveju valstybės narės turėtų taikyti tokių konkretiems sektoriams taikomų Sąjungos teisės aktų nuostatas, be kita ko, susijusias su jurisdikcija, ir neturėtų vykdyti esminių paslaugų operatorių identifikavimo proceso, nustatyto šia direktyva. Šiomis aplinkybėmis valstybės narės turėtų Komisijai teikti informaciją apie tokių *lex specialis* nuostatų taikymą. Nustatant, ar reikalavimai dėl tinklų ir informacinių sistemų saugumo ir pranešimų apie incidentus, įtraukti į konkretiems sektoriams taikomus Sąjungos teisės aktus, yra lygiaverčiai reikalavimams, nustatytiems šioje direktyvoje, reikėtų atsižvelgti tik į atitinkamų Sąjungos teisės aktų nuostatas ir jų taikymą valstybėse narėse;

(10) vandens transporto sektoriuje saugumo reikalavimai, taikomi bendrovėms, laivams, uostų įrenginiams, uostų ir laivų eismo valdymo paslaugoms, pagal Sąjungos teisės aktus apima visas operacijas, įskaitant radijo ir telekomunikacijų sistemas, kompiuterių sistemas ir tinklus. Dalis privalomų procedūrų, kurių turi būti laikomasi, apima pranešimą apie visus saugumo incidentus ir todėl turėtų būti laikomos *lex specialis* tiek, kiek tie reikalavimai yra bent lygiaverčiai atitinkamoms šios direktyvos nuostatoms;

([1]) 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva 2002/21/EB dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos (Pagrindų direktyva) (OL L 108, 2002 4 24, p. 33).

([2]) 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB (OL L 257, 2014 8 28, p. 73).

([3]) 2013 m. rugsėjo 23 d. Tarybos sprendimas 2013/488/ES dėl ES įslaptintos informacijos apsaugai užtikrinti skirtų saugumo taisyklių (OL L 274, 2013 10 15, p. 1).

(11) identifikuodamos operatorius vandens transporto sektoriuje, valstybės narės turėtų atsižvelgti į galiojančius ir būsimus tarptautinius kodeksus ir gaires, kuriuos visų pirma parengia Tarptautinė jūrų organizacija, kad atskirų jūrų laivybos operatorių atžvilgiu būtų laikomasi nuoseklaus požiūrio;

(12) bankininkystės ir finansų rinkos infrastruktūros objektų sektorių reglamentavimas ir priežiūra yra gerai suderinti Sąjungos lygmeniu Sąjungos pirminės ir antrinės teisės pagalba bei naudojant standartus, parengtus kartu su Europos priežiūros institucijomis. Bankų sąjungoje tų reikalavimų taikymas ir priežiūra užtikrinami bendru priežiūros mechanizmu. Valstybėse narėse, kurios nėra bankų sąjungos narės, tai užtikrina atitinkamos valstybių narių bankų reguliavimo institucijos. Kitose finansų sektoriaus reglamentavimo srityse Europos finansų priežiūros institucijų sistema taip pat užtikrina aukštą priežiūros praktikos bendrumo ir konvergencijos lygį. Europos vertybinių popierių ir rinkų institucija taip pat vykdo tam tikrų subjektų, t. y. kredito reitingų agentūrų ir sandorių duomenų saugyklų, tiesioginės priežiūros funkciją;

(13) operacinė rizika yra itin svarbi bankininkystės ir finansų rinkų infrastruktūros objektų sektorių prudencinio reguliavimo ir priežiūros dalis. Tai apima visas operacijas, įskaitant tinklų ir informacinių sistemų saugumą, vientisumą ir atsparumą. Toms sistemoms taikomi reikalavimai, kurie dažnai yra griežtesni už pagal šią direktyvą numatytus reikalavimus, yra nustatyti tam tikruose Sąjungos teisės aktuose, įskaitant: taisykles dėl galimybės verstis kredito įstaigų veikla ir dėl kredito įstaigų ir investicinių įmonių prudencinės priežiūros; taisykles dėl prudencinių reikalavimų kredito įstaigoms ir investicinėms įmonėms, kurios apima reikalavimus dėl operacinės rizikos; taisykles dėl finansinių priemonių rinkų, kurios apima reikalavimus dėl investicinių įmonių ir reguliuojamų rinkų rizikos vertinimo; taisykles dėl ne biržos išvestinių finansinių priemonių, pagrindinių sandorio šalių ir sandorių duomenų saugyklų, kurios apima reikalavimus dėl pagrindinių sandorio šalių ir sandorių duomenų saugyklų operacinės rizikos; taisykles dėl atsiskaitymo už vertybinius popierius gerinimo Sąjungoje ir centrinių vertybinių popierių depozitoriumų, kurios apima reikalavimus dėl operacinės rizikos. Be to, pranešimų apie incidentus reikalavimai yra įprastos finansų sektoriaus priežiūros praktikos dalis ir dažnai įtraukiami į priežiūros vadovus. Valstybės narės turėtų į tas taisykles ir reikalavimus atsižvelgti taikydamos *lex specialis*;

(14) kaip nurodyta 2014 m. liepos 25 d. Europos Centrinio Banko nuomonėje ([1]), ši direktyva nepažeidžia pagal Sąjungos teisę taikomo Eurosistemos mokėjimo ir atsiskaitymo sistemų priežiūros režimo. Už tokią priežiūrą atsakingoms institucijoms ir pagal šią direktyvą kompetentingoms institucijoms būtų tikslinga keistis patirtimi su tinklų ir informacinių sistemų saugumu susijusiais klausimais. Tas pats taikytina Europos centrinių bankų sistemos euro zonai nepriklausantiems nariams, kurie vykdo tokią mokėjimo ir atsiskaitymo sistemų priežiūrą remdamiesi nacionaliniais įstatymais ir kitais teisės aktais;

(15) elektroninėje prekyvietėje vartotojams ir komercinės veiklos subjektams leidžiama sudaryti elektroninės prekybos arba paslaugų sutartis su komercinės veiklos subjektais, ir ši prekyvietė yra tokių sutarčių sudarymo galutinė paskirties vieta. Ji neturėtų apimti internetinių paslaugų, teikiamų tik tarpininkaujant trečiųjų šalių paslaugų atžvilgiu, kai galiausiai galima sudaryti sutartį. Todėl ji neturėtų apimti internetinių paslaugų, kurias teikiant lyginama skirtingų komercinės veiklos subjektų tiekiamų konkrečių produktų ar teikiamų konkrečių paslaugų kaina ir tada naudotojas nukreipiamas į pageidautiną komercinės veiklos subjektą, kad įsigytų produktą. Elektroninėje prekyvietėje teikiamos kompiuterijos paslaugos gali apimti sandorių tvarkymą, duomenų kaupimą ar naudotojų profiliavimą. Taikomųjų programų parduotuvės, kurios veikia kaip elektroninės parduotuvės, kuriose sudaromos sąlygos skaitmeniniam trečiųjų šalių programų ar programinės įrangos platinimui, turi būti laikomos internetinės prekyvietės rūšimi;

(16) interneto paieškos sistema leidžia naudotojui vykdyti paiešką iš esmės visose svetainėse remiantis bet kurio dalyko užklausa. Be to, ši sistema gali būti tikslingai nukreipta į svetaines konkrečia kalba. Šioje direktyvoje nustatyta interneto paieškos sistemos apibrėžtis neturėtų apimti paieškos funkcijų, kurios apsiriboja konkrečios svetainės turiniu, nepriklausomai nuo to, ar paieškos funkcija yra numatyta išorinėje paieškos sistemoje. Ji taip pat neturėtų apimti internetinių paslaugų, kurias teikiant lyginama skirtingų komercinės veiklos subjektų tiekiamų konkrečių produktų ar teikiamų konkrečių paslaugų kaina ir tada naudotojas nukreipiamas į pageidaujamą komercinės veiklos subjektą, kad įsigytų produktą;

(17) debesijos kompiuterijos paslaugos apima įvairiausią veiklą, kuri gali būti vykdoma pagal įvairius modelius. Šioje direktyvoje terminas „debesijos kompiuterijos paslaugos“ apima paslaugas, kurios suteikia prieigą prie kintamo masto pritaikomos bendrų kompiuterijos išteklių bazės. Tie kompiuterijos ištekliai apima tokius išteklius, kaip antai tinklai, serveriai ar kita infrastruktūra, kaupikliai, taikomosios programos ir paslaugos. Terminas „kintamo masto“ reiškia, kad siekdamas atsižvelgti į paklausos svyravimus, debesijos paslaugų teikėjas lanksčiai paskirsto kompiuterijos išteklius nepriklausomai nuo geografinės išteklių vietos. Terminas „pritaikoma bazė“ reiškia, kad

([1]) OL C 352, 2014 10 7, p. 4.

siekiant sparčiai padidinti ir sumažinti tuos turimus kompiuterijos išteklius pagal darbo krūvį, tais ištekliais aprūpinama ir jie yra tiekiami atsižvelgiant į paklausą. Terminas „bendras“ reiškia, kad tie kompiuterijos ištekliai yra tiekiami įvairiems naudotojams, kurie dalijasi bendra prieiga prie paslaugos, tačiau tie ištekliai tvarkomi atskirai kiekvieno naudotojo atveju, nors paslauga yra teikiama naudojant tą pačią elektroninę įrangą;

(18) interneto duomenų srautų mainų taško (toliau – IXP) funkcija yra tinklų sujungimas. IXP nesuteikia prieigos prie tinklo ir nėra persiuntimo paslaugų teikėjas ar nešlys. Be to, IXP neteikia kitų su sujungimu nesusijusių paslaugų, tačiau tai nekliudo IXP operatoriui teikti nesusijusias paslaugas. IXP egzistuoja tam, kad būtų sujungti tinklai, kurie techniniu ir organizavimo požiūriu yra atskiri. Techniniu požiūriu atskiram tinklui apibūdinti vartojamas terminas „autonominė sistema“;

(19) valstybės narės turėtų būti atsakingos už tai, kad būtų nustatyta, kurie subjektai tenkina esminių paslaugų operatoriaus apibrėžties kriterijus. Siekiant užtikrinti, kad būtų laikomasi nuoseklaus požiūrio, esminių paslaugų operatoriaus apibrėžtis turėtų būti nuosekliai taikoma visos valstybėse narėse. Tuo tikslu šioje direktyvoje numatomas konkrečiuose sektoriuose ir subsektoriuose veiklą vykdančių subjektų vertinimas, esminių paslaugų sąrašo sudarymas, tarpsektorinių veiksnių, kuriais remiantis nustatoma, ar galimas incidentas turėtų didelį trikdomąjį poveikį, bendro sąrašo svarstymas, konsultavimosi procesas, kuriame dalyvautų atitinkamos valstybės narės tuo atveju, kai subjektai teikia paslaugas daugiau nei vienoje valstybėje narėje, ir Bendradarbiavimo grupės parama identifikavimo procese. Siekdamos užtikrinti, kad būtų tiksliai atspindėti galimi pokyčiai rinkoje, valstybės narės turėtų reguliariai peržiūrėti nustatytų operatorių sąrašą ir prireikus jį atnaujinti. Galiausiai valstybės narės turėtų pateikti Komisijai informaciją, būtiną siekiant įvertinti, kokiu mastu dėl šios bendros metodikos valstybės narės galėjo nuosekliai taikyti apibrėžtį;

(20) esminių paslaugų operatorių identifikavimo proceso metu valstybės narės turėtų įvertinti, kurios paslaugos, bent kiekvieno šioje direktyvoje nurodyto sektoriaus atveju, turi būti laikomos būtinomis siekiant užtikrinti ypatingos svarbos visuomeninės ir ekonominės veiklos vykdymą, ir ar subjektai, kurie vykdo veiklą šioje direktyvoje išvardytuose sektoriuose bei subsektoriuose ir kurie teikia tas paslaugas, tenkina operatorių identifikavimo kriterijus. Nustatant, ar subjektas teikia paslaugą, kuri yra būtina siekiant užtikrinti ypatingos svarbos visuomeninės ar ekonominės veiklos vykdymą, pakanka ištirti, ar tas subjektas teikia paslaugą, kuri yra įtraukta į esminių paslaugų sąrašą. Be to, turėtų būti įrodyta, kad esminės paslaugos teikimas priklauso nuo tinklų ir informacinių sistemų. Galiausiai nustatydamos, ar incidentas turėtų didelį trikdomąjį poveikį paslaugos teikimui, valstybės narės turėtų atsižvelgti į tam tikrus tarpsektorinius veiksnius, taip pat, prireikus, į konkretiems sektoriams būdingus veiksnius;

(21) identifikuojant esminių paslaugų operatorius, įsteigimas valstybėje narėje reiškia, kad jie veiksmingai vykdo realią veiklą remdamiesi stabiliomis struktūromis. Teisinė tokių struktūrų forma, neatsižvelgiant į tai, ar tai yra filialas, ar patronuojamoji bendrovė, turinti juridinio asmens statusą, šiuo požiūriu nėra lemiamas veiksnys;

(22) šioje direktyvoje nurodytuose sektoriuose ir subsektoriuose veikiantys subjektai gali teikti tiek esmines, tiek neesmines paslaugas. Pavyzdžiui, oro transporto sektoriuje oro uostai gali teikti paslaugas, kurias valstybės narės gali laikyti esminėmis, kaip antai kilimo ir tūpimo takų valdymo paslaugas, tačiau taip pat tam tikras paslaugas, kurios gali būti laikomos neesminėmis, kaip antai prekybos zonų administravimo paslaugas. Esminių paslaugų operatoriams turėtų būti taikomi konkretūs saugumo reikalavimai tik tų paslaugų, kurios laikomos esminėmis, atžvilgiu. Todėl, siekdamos identifikuoti operatorius, valstybės narės turėtų sudaryti paslaugų, kurios laikomos esminėmis, sąrašą;

(23) į paslaugų sąrašą turėtų būti įtrauktos visos paslaugos, teikiamos atitinkamos valstybės narės teritorijoje, kurios atitinka pagal šią direktyvą nustatytus reikalavimus. Valstybės narės turėtų turėti galimybę į galiojantį sąrašą įtraukti naujas paslaugas. Paslaugų sąrašas turėtų tapti valstybių narių atskaitos tašku identifikuojant esminių paslaugų operatorius. Jo paskirtis – padėti identifikuoti esminių paslaugų rūšis bet kuriame konkrečiame šioje direktyvoje nurodytame sektoriuje, tokiu būdu atskiriant jas nuo neesminių paslaugų, už kurias gali būti atsakingas konkrečiame sektoriuje veiklą vykdantis subjektas. Kiekvienos valstybės narės sudarytu paslaugų sąrašu turėtų būti remiamasi vėliau vertinant reglamentavimo praktiką kiekvienoje valstybėje narėje siekiant užtikrinti bendrą identifikavimo proceso nuoseklumo lygį valstybėse narėse;

(24) identifikavimo proceso tikslais, kai subjektas teikia esminę paslaugą dviejose ar daugiau valstybių narių, tos valstybės narės turėtų tarpusavyje vesti dvišales arba daugiašales diskusijas. Šio konsultavimosi proceso tikslas – padėti joms įvertinti operatoriaus ypatingą svarbą tarpvalstybinio poveikio požiūriu ir taip sudaryti kiekvienai dalyvaujančiai valstybei narei galimybę pateikti savo nuomonę dėl rizikos, susijusios su teikiamomis paslaugomis. Atitinkamos valstybės narės turėtų atsižvelgti į viena kitos nuomones šiame procese ir šiuo tikslu jos turėtų turėti galimybę prašyti Bendradarbiavimo grupės paramos;

(25) vykdydamos identifikavimo procesą valstybės narės turėtų patvirtinti nacionalines priemones, kuriomis remiantis būtų nustatyti subjektai, kuriems turi būtų taikomos tinklų ir informacinių sistemų saugumo pareigos. Tai galėtų būti pasiekta priimant sąrašą, kuriame būtų išvardyti visi esminių paslaugų operatoriai, arba patvirtinant nacionalines priemones, įskaitant objektyvius kiekybiškai įvertinamus kriterijus, kaip antai operatoriaus veiklos apimtį arba naudotojų skaičių, kuriais remiantis būtų galima nustatyti subjektus, kuriems taikomos tinklų ir informacinių sistemų saugumo pareigos. Nacionalinės priemonės, neatsižvelgiant į tai, ar jos jau galioja ar yra patvirtintos remiantis šia direktyva, turėtų apimti visas teisines priemones, administracines ir politines priemones, kuriomis remiantis galima identifikuoti esminių paslaugų operatorius pagal šią direktyvą;

(26) siekdamos nuspręsti, ar identifikuoti esminių paslaugų operatoriai yra svarbūs atitinkamam sektoriui, valstybės narės turėtų atsižvelgti į tų operatorių skaičių ir dydį, pavyzdžiui, į jų rinkos dalį arba pagamintų produktų ar teikiamų paslaugų kiekį, neįpareigojant atskleisti informacijos, kuri rodytų, kurie operatoriai buvo identifikuoti;

(27) siekdamos nustatyti, ar incidentas padarytų didelį trikdomąjį poveikį esminės paslaugos teikimui, valstybės narės turėtų atsižvelgti į tam tikrus įvairius veiksnius, kaip antai į vartotojų, kurie naudojasi ta paslauga privačiais arba profesiniais tikslais, skaičių. Ta paslauga gali būti naudojamasi tiesiogiai, netiesiogiai arba per tarpininką. Nustatydamos poveikį, kurį incidentas dėl savo masto ir trukmės galėtų padaryti ekonominei ir visuomeninei veiklai arba viešajam saugumui, valstybės narės taip pat turėtų įvertinti, kiek laiko gali praeiti, kol paslaugos teikimo sutrikimas pradėtų daryti neigiamą poveikį;

(28) siekiant nustatyti, ar incidentas padarytų didelį trikdomąjį poveikį esminės paslaugos teikimui, turėtų būti atsižvelgta ne tik į tarpsektorinius veiksnius, bet ir į konkretiems sektoriams būdingus veiksnius. Energijos tiekėjų atveju tokie veiksniai galėtų apimti pagamintos nacionalinės energijos kiekį arba jos dalį, naftos tiekėjų atveju – kiekį per dieną, oro transporto (įskaitant oro uostus ir oro vežėjus), geležinkelių transporto ir jūrų uostų atveju – nacionalinio eismo intensyvumo dalį ir keleivių arba krovinių vežimo operacijų skaičių per metus, bankų arba finansų rinkos infrastruktūros objektų atveju – jų sisteminę svarbą, grindžiamą visu turtu arba to viso turto santykine BVP dalimi, sveikatos apsaugos sektoriaus atveju – sveikatos priežiūros paslaugų teikėjo pacientų skaičių per metus, vandens gamybos, perdirbimo ir tiekimo atveju – vandens kiekį ir vartotojų, kuriems vanduo tiekiamas, skaičių ir rūšis, įskaitant, pavyzdžiui, ligonines, viešąsias paslaugas, organizacijas ar fizinius asmenis, taip pat alternatyvių vandens išteklių egzistavimą siekiant aptarnauti tą pačią geografinę vietovę;

(29) norėdama pasiekti ir išlaikyti aukštą tinklų ir informacinių sistemų saugumo lygį, kiekviena valstybė narė turėtų turėti nacionalinę tinklų ir informacinių sistemų saugumo strategiją, kurioje būtų apibrėžti strateginiai tikslai ir konkretūs politikos veiksmai, kuriuos reikia įgyvendinti;

(30) atsižvelgiant į nacionalinių valdymo struktūrų skirtumus ir siekiant išsaugoti jau veikiančias sektorių sistemas ar Sąjungos priežiūros ir reguliavimo įstaigas bei išvengti dubliavimo, valstybės narės turėtų turėti teisę paskirti daugiau nei vieną nacionalinę kompetentingą instituciją, atsakingą už užduočių, susijusių su esminių paslaugų operatorių bei skaitmeninių paslaugų teikėjų tinklų ir informacinių sistemų saugumu, vykdymą pagal šią direktyvą;

(31) siekiant palengvinti tarpvalstybinį bendradarbiavimą ir ryšių palaikymą bei sudaryti sąlygas veiksmingai įgyvendinti šią direktyvą, būtina, kad kiekviena valstybė narė, nedarydama poveikio sektoriniams reguliavimo susitarimams, paskirtų nacionalinį bendrąjį informacinį centrą, atsakingą už klausimų, susijusių su tinklų ir informacinių sistemų saugumu, koordinavimą ir tarpvalstybinį bendradarbiavimą Sąjungos lygmeniu. Kompetentingos institucijos ir bendrieji informaciniai centrai turėtų turėti pakankamai techninių, finansinių ir žmogiškųjų išteklių, siekiant užtikrinti, kad jie galėtų veiksmingai ir efektyviai vykdyti jiems pavestas užduotis ir taip įgyvendinti šios direktyvos tikslus. Kadangi šia direktyva siekiama gerinti vidaus rinkos veikimą užtikrinant atsakomybę ir tarpusavio pasitikėjimą, valstybių narių įstaigos turi galėti veiksmingai bendradarbiauti su ekonominės veiklos vykdytojais ir būti atitinkamos struktūros;

(32) kompetentingos institucijos arba reagavimo į kompiuterių saugumo incidentus tarnybos (toliau – CSIRT) turėtų gauti pranešimus apie incidentus. Bendrieji informaciniai centrai neturėtų tiesiogiai gauti pranešimų apie incidentus, nebent jie taip pat veiktų kaip kompetentinga institucija arba CSIRT. Tačiau kompetentinga institucija arba CSIRT galėtų pavesti bendrajam informaciniam centrui perduoti pranešimus apie incidentus kitų paveiktų valstybių narių bendriesiems informaciniams centrams;

(33) siekiant užtikrinti veiksmingą informacijos teikimą valstybėms narėms ir Komisijai, bendrojo informacinio centro Bendradarbiavimo grupei pateikta suvestinė ataskaita turėtų būti nuasmeninta siekiant išsaugoti pranešimų konfidencialumą ir esminių paslaugų operatorių bei skaitmeninių paslaugų teikėjų tapatybę, nes keičiantis geriausia praktika Bendradarbiavimo grupėje nereikalaujama informacijos apie pranešančiųjų subjektų tapatybę. Į suvestinę ataskaitą turėtų būti įtraukta informacija apie gautų pranešimų skaičių, taip pat nurodytas praneštų incidentų pobūdis, kaip antai saugumo pažeidimų rūšys, jų rimtumas ar jų trukmė;

(34) valstybės narės turėtų būti tinkamai pasirengusios – turėti tiek techninių, tiek organizacinių pajėgumų, kad galėtų išvengti su tinklų ir informacinėmis sistemomis susijusių incidentų bei rizikos, juos nustatyti, į juos reaguoti ir sušvelninti jų poveikį. Todėl valstybės narės turėtų užtikrinti, kad jose būtų gerai veikiančios CSIRT, dar vadinamos reagavimo į kompiuterių incidentus tarnybos, atitinkančios esminius reikalavimus, kad būtų garantuoti veiksmingi bei suderinami incidentų bei rizikos valdymo pajėgumai ir užtikrintas veiksmingas bendradarbiavimas Sąjungos lygmeniu. Siekdamos, kad visų rūšių esminių paslaugų operatoriai ir skaitmeninių paslaugų teikėjai galėtų pasinaudoti tokiais pajėgumais ir bendradarbiavimu, valstybės narės turėtų užtikrinti, kad paskirtasis CSIRT į savo veiklą įtrauktų visas operatorių ir teikėjų rūšis. Atsižvelgiant į tarptautinio bendradarbiavimo kibernetinio saugumo srityje svarbą, CSIRT turėti galimybę dalyvauti ne tik šia direktyva sukurto CSIRT tinklo, bet ir tarptautinio bendradarbiavimo tinklų veikloje;

(35) kadangi daugumą tinklų ir informacinių sistemų valdo privatūs operatoriai, labai svarbus viešojo ir privačiojo sektorių bendradarbiavimas. Esminių paslaugų operatoriai ir skaitmeninių paslaugų teikėjai turėtų būti skatinami taikyti savo neformalius bendradarbiavimo mechanizmus, kad užtikrintų tinklų ir informacinių sistemų saugumą. Bendradarbiavimo grupė turėtų galėti prireikus į diskusijas pakviesti atitinkamų suinteresuotųjų subjektų. Siekiant veiksmingai skatinti dalytis informacija ir geriausia praktika, itin svarbu užtikrinti, kad tokiuose mainuose dalyvaujantys esminių paslaugų operatoriai ir skaitmeninių paslaugų teikėjai dėl tarpusavio bendradarbiavimo neatsidurtų nepalankesnėje padėtyje;

(36) ENISA turėtų padėti valstybėms narėms ir Komisijai teikti ekspertines žinias, konsultuoti ir palengvinti keitimąsi geriausia praktika. Visų pirma, taikant šią direktyvą, Komisija turėtų, o valstybės narės turėtų galėti konsultuotis su ENISA. Siekiant stiprinti valstybių narių gebėjimus ir žinias, Bendradarbiavimo grupė taip pat turėtų tapti keitimosi geriausia praktika, diskusijų dėl pajėgumų bei valstybių narių parengties priemone ir savanoriškai padėti savo nariams vertinti nacionalines tinklų ir informacinių sistemų saugumo strategijas, stiprinti gebėjimus ir vykdyti pratybų, susijusių su tinklų ir informacinių sistemų saugumu, vertinimus;

(37) valstybės narės, taikydamos šią direktyvą, prireikus turėtų turėti teisę naudoti ar pritaikyti esamas organizacines struktūras ar strategijas;

(38) atitinkamos Bendradarbiavimo grupės ir ENISA užduotys yra tarpusavyje susijusios ir viena kitą papildančios. Iš esmės ENISA turėtų padėti Bendradarbiavimo grupei vykdyti savo užduotis vadovaujantis ENISA tikslu, nustatytu Europos Parlamento ir Tarybos reglamente (ES) Nr. 526/2013 ([1]), t. y. padėti Sąjungos institucijoms, įstaigoms, tarnyboms ir agentūroms ir valstybėms narėms įgyvendinti politiką, būtiną įgyvendinti tinklų ir informacinių sistemų saugumo teisinius ir norminius reikalavimus, nustatytus esamuose ir būsimuose Sąjungos teisės aktuose. Visų pirma ENISA turėtų teikti pagalbą tose srityse, kurios atitinka jos pačios užduotis, kaip nustatyta Reglamente (ES) Nr. 526/2013, t. y. analizuoti tinklų ir informacinių sistemų saugumo strategijas, remti Sąjungos pratybų, susijusių su tinklų ir informacinių sistemų saugumu, organizavimą bei jas vykdyti, taip pat keistis informacija ir geriausia praktika informuotumo didinimo ir mokymo srityje. Be to, ENISA turėtų dalyvauti rengiant gaires dėl konkretiems sektoriams taikomų kriterijų, kuriais remiantis nustatomas incidento poveikio mastas;

([1]) 2013 m. gegužės 21 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 526/2013 dėl Europos Sąjungos tinklų ir informacijos apsaugos agentūros (ENISA), kuriuo panaikinamas Reglamentas (EB) Nr. 460/2004 (OL L 165, 2013 6 18, p. 41).

(39) siekdama skatinti didesnį tinklų ir informacinių sistemų saugumą, Bendradarbiavimo grupė turėtų prireikus bendradarbiauti su atitinkamomis Sąjungos institucijomis, įstaigomis, tarnybomis ir agentūromis, kad būtų keičiamasi praktine patirtimi ir geriausia praktika, konsultuojamasi dėl tinklų ir informacinių sistemų saugumo aspektų, kurie gali turėti įtakos jų darbui, kartu laikantis galiojančių susitarimų dėl keitimosi riboto naudojimo informacija. Bendradarbiaudama su teisėsaugos įstaigomis dėl tinklų ir informacinių sistemų saugumo aspektų, kurie gali turėti įtakos jų darbui, Bendradarbiavimo grupė turėtų atsižvelgti į veikiančius informacijos kanalus ir sukurtus tinklus;

(40) informacija apie incidentus tampa vis vertingesnė plačiajai visuomenei ir įmonėms, visų pirma mažosioms ir vidutinėms įmonėms. Kai kuriais atvejais tokia informacija jau yra teikiama svetainėse nacionaliniu lygmeniu konkrečios šalies kalba, daugiausia dėmesio skiriant nacionalinio masto incidentams ir jų atvejų skaičiui. Atsižvelgiant į tai, kad įmonės vis dažniau vykdo tarpvalstybinę veiklą, o piliečiai naudojasi internetinėmis paslaugomis, informacija apie incidentus turėtų būti teikiama apibendrinta forma Sąjungos lygmeniu. CSIRT tinklo sekretoriatas raginamas tvarkyti svetainę arba suteikti prieglobą specialiam veikiančios svetainės puslapiui, kuriuose plačioji visuomenė galėtų rasti bendro pobūdžio informacijos apie didelio masto bet kur Sąjungoje įvykusius incidentus, kuriuose ypač daug dėmesio būtų skiriama įmonių interesams ir poreikiams. CSIRT tinkle dalyvaujančios CSIRT raginamos savanoriškai teikti informaciją, kuri būtų skelbiama toje svetainėje, neįtraukiant konfidencialios arba neskelbtinos informacijos;

(41) kai pagal Sąjungos ir nacionalines verslo konfidencialumo taisykles informacija laikoma konfidencialia, toks konfidencialumas turėtų būti užtikrintas vykdant šioje direktyvoje numatytą veiklą ir įgyvendinant jos tikslus;

(42) norinti patikrinti valstybių narių parengtį ir bendradarbiavimą itin svarbios kibernetinio saugumo pratybos, kuriose simuliuojami incidentų scenarijai tikruoju laiku. ENISA koordinuojamas *CyberEurope* pratybų ciklas, kuriame dalyvauja valstybės narės, yra naudinga patikrinimo priemonė ir rekomendacijų dėl tolesnio reagavimo į incidentus Sąjungos lygmeniu tobulinimo rengimo priemonė. Atsižvelgiant į tai, kad valstybės narės šiuo metu nėra įpareigotos planuoti pratybų ar jose dalyvauti, pagal šią direktyvą sukūrus CSIRT tinklą valstybėms narėms turėtų būti sudarytos sąlygos dalyvauti pratybose remiantis tiksliu planavimu ir strateginiais sprendimais. Pagal šią direktyvą įsteigta Bendradarbiavimo grupė turėtų būti atsakinga už strateginius sprendimus, susijusius su pratybomis, ypač, bet ne vien, su tų pratybų reguliarumu ir scenarijų projektais. ENISA, vadovaudamasi savo įgaliojimais, turėtų remti Sąjungos masto pratybų organizavimą ir vykdymą Bendradarbiavimo grupei ir CSIRT tinklui teikdama ekspertines žinias ir konsultacijas;

(43) atsižvelgiant į visuotinį saugumo problemų, kurios daro poveikį tinklų ir informacinėms sistemoms, pobūdį, reikalingas glaudesnis tarptautinis bendradarbiavimas siekiant pagerinti saugumo standartus bei keitimąsi informacija ir skatinti bendrą visuotinį požiūrį į saugumo klausimus;

(44) atsakomybė už tinklų ir informacinių sistemų saugumo užtikrinimą didžia dalimi tenka esminių paslaugų operatoriams ir skaitmeninių paslaugų teikėjams. Rizikos valdymo kultūra, apimanti rizikos vertinimą ir esamą riziką atitinkančių saugumo priemonių įgyvendinimą, turėtų būti skatinama ir plėtojama taikant atitinkamus reglamentavimo reikalavimus ir savanorišką sektorių praktiką. Siekiant užtikrinti veiksmingą visų valstybių narių bendradarbiavimą, patikimų vienodų veiklos sąlygų sudarymas taip pat yra esminis veiksnys veiksmingam Bendradarbiavimo grupės ir CSIRT tinklo veikimui;

(45) ši direktyva taikoma tik toms viešojo administravimo institucijoms, kurios yra identifikuotos kaip esminių paslaugų operatoriai. Todėl valstybės narės turi užtikrinti viešojo administravimo institucijų, kurios nepatenka į šios direktyvos taikymo sritį, tinklų ir informacinių sistemų saugumą;

(46) rizikos valdymo priemonės apima priemones, skirtas incidentų rizikai nustatyti, incidentų prevencijos, nustatymo, valdymo ir jų poveikio švelninimo priemones. Tinklų ir informacinių sistemų saugumas apima saugomų, perduodamų ir tvarkomų duomenų saugumą;

(47) kompetentingos institucijos turėtų išlaikyti teisę priimti nacionalines gaires dėl aplinkybių, kuriomis reikalaujama, kad esminių paslaugų operatoriai praneštų apie incidentus;

(48) daugelio įmonių paslaugų teikimas Sąjungoje priklauso nuo skaitmeninių paslaugų teikėjų. Kadangi kai kurios skaitmeninės paslaugos gali būti svarbus jų naudotojų, įskaitant esminių paslaugų operatorius, išteklius ir kadangi tokie naudotojai ne visada gali turėti alternatyvų, ši direktyva taip pat turėtų būti taikoma tokių paslaugų teikėjams. Šioje direktyvoje nurodytos rūšies skaitmeninių paslaugų saugumas, tęstinumas ir patikimumas yra itin svarbūs sklandžiam daugelio įmonių veikimui. Dėl tokios skaitmeninės paslaugos sutrikdymo būtų neįmanoma teikti kitų paslaugų, kurios priklauso nuo šios paslaugos, ir todėl būtų padarytas poveikis pagrindinei ekonominei ir visuomeninei veiklai Sąjungoje. Todėl tokios skaitmeninės paslaugos gali būti ypač svarbios sklandžiam įmonių, kurios nuo šių paslaugų priklauso, veikimui ir dar labiau – tokių įmonių dalyvavimui vidaus rinkoje ir tarpvalstybinėje prekyboje visoje Sąjungoje. Į šios direktyvos taikymo sritį įtraukti skaitmeninių paslaugų teikėjai yra tie teikėjai, kurie siūlo skaitmenines paslaugas, nuo kurių vis labiau priklauso daugelis įmonių Sąjungoje;

(49) skaitmeninių paslaugų teikėjai turėtų užtikrinti tokį saugumo lygį, kuris būtų proporcingas jų teikiamų skaitmeninių paslaugų saugumui kylančios rizikos laipsniui, atsižvelgiant į jų paslaugų svarbą kitų įmonių operacijoms Sąjungoje. Praktiškai esminių paslaugų, kurios dažnai turi esminę reikšmę užtikrinant visuomenei ir ekonomikai būtiniausią veiklą, operatoriams kylančios rizikos laipsnis yra didesnis už skaitmeninių paslaugų teikėjams kylančios rizikos laipsnį. Todėl skaitmeninių paslaugų teikėjams keliami saugumo reikalavimai turėtų būti mažiau griežti. Skaitmeninių paslaugų teikėjai turėtų išlaikyti teisę imtis priemonių, kurios, jų nuomone, yra tinkamos siekiant valdyti jų tinklų ir informacinių sistemų saugumui kylančią riziką. Dėl skaitmeninių paslaugų tarpvalstybinio pobūdžio jų teikėjams turėtų būti taikomas Sąjungos lygmeniu labiau suderintas požiūris. Įgyvendinimo aktais turėtų būti palengvintas tokių priemonių tikslus apibrėžimas ir įgyvendinimas;

(50) nors aparatinės įrangos gamintojai ir programinės įrangos kūrėjai nėra esminių paslaugų operatoriai ar skaitmeninių paslaugų teikėjai, panašūs į tuos, kuriems taikoma ši direktyva, jų produktai padidina tinklų ir informacinių sistemų saugumo užtikrinimą. Todėl jiems tenka svarbus vaidmuo sudarant esminių paslaugų operatoriams ir skaitmeninių paslaugų teikėjams sąlygas apsaugoti savo tinklų ir informacinės infrastruktūros objektus. Tokiems aparatinės ir programinės įrangos produktams jau taikomos galiojančios taisyklės dėl atsakomybės už gaminius;

(51) esminių paslaugų operatoriams ir skaitmeninių paslaugų teikėjams taikomomis techninėmis ir organizacinėmis priemonėmis neturėtų būti reikalaujama, kad konkretus komercinis informacinių ir ryšių technologijų produktas būtų suprojektuotas, sukurtas ar pagamintas tam tikru būdu;

(52) esminių paslaugų operatoriai ir skaitmeninių paslaugų teikėjai turėtų užtikrinti jų naudojamų tinklų ir informacinių sistemų saugumą. Tai visų pirma būtų privatūs tinklai ir informacinės sistemos, kurias administruoja jų vidaus IT personalas arba kurių saugumas užtikrinamas veiklos ranga. Saugumo ir pranešimų teikimo reikalavimai turėtų būti taikomi atitinkamiems esminių paslaugų operatoriams ir skaitmeninių paslaugų teikėjams, nepriklausomai nuo to, ar savo tinklų ir informacinių sistemų techninę priežiūrą jie vykdo patys ar veiklos rangos būdu;

(53) siekiant neužkrauti neproporcingos finansinės ir administracinės naštos esminių paslaugų operatoriams ir skaitmeninių paslaugų teikėjams, reikalavimai turėtų būti proporcingi rizikai, kurią kelia atitinkama tinklų ir informacinė sistema, atsižvelgiant į tokių priemonių modernumą. Skaitmeninių paslaugų teikėjų atveju tie reikalavimai neturėtų būti taikomi labai mažoms ir mažosioms įmonėms;

(54) kai viešojo administravimo institucijos valstybėse narėse naudojasi skaitmeninių paslaugų teikėjų teikiamomis paslaugomis, visų pirma debesijos kompiuterijos paslaugomis, jos gali norėti reikalauti, kad tokių paslaugų teikėjai suteiktų papildomų saugumo priemonių, kuriomis būtų papildytos priemonės, kurias skaitmeninių paslaugų teikėjai paprastai siūlo laikydamiesi šios direktyvos reikalavimų. Jos tai galėtų padaryti remdamosi sutartinėmis pareigomis;

(55) šioje direktyvoje elektroninių prekyviečių, interneto paieškos sistemų ir debesijos kompiuterijos paslaugų apibrėžtys yra taikomos tik konkrečiu šios direktyvos tikslu ir nedaro poveikio kitoms priemonėms;

(56) šia direktyva neturėtų būti kliudoma valstybėms narėms patvirtinti nacionalines priemones, kuriomis viešojo sektoriaus įstaigos būtų įpareigotos užtikrinti konkrečių saugumo reikalavimų laikymąsi užsakant debesijos kompiuterijos paslaugas. Tokios nacionalinės priemonės turėtų būti taikomos atitinkamai viešojo sektoriaus įstaigai, o ne debesijos kompiuterijos paslaugų teikėjui;

(57) atsižvelgiant į esminius skirtumus tarp esminių paslaugų operatorių, visų pirma jų tiesioginį ryšį su fizine infrastruktūra, ir skaitmeninių paslaugų teikėjų, visų pirma jų paslaugų tarpvalstybinį pobūdį, šioje direktyvoje turėtų būti laikomasi diferencijuoto požiūrio į suderinimo lygį abiejų šių subjektų grupių atžvilgiu. Valstybės narės turėtų turėti teisę identifikuoti atitinkamus esminių paslaugų operatorius ir taikyti griežtesnius reikalavimus nei nustatytieji šioje direktyvoje. Valstybės narės neturėtų identifikuoti skaitmeninių paslaugų teikėjų, nes ši direktyva turėtų būti taikoma visiems skaitmeninių paslaugų teikėjams, patenkantiems į jos taikymo sritį. Be to, šia direktyva ir pagal ją priimtais įgyvendinimo aktais turėtų būti užtikrintas aukštas suderinimo lygis skaitmeninių paslaugų teikėjams taikomų saugumo ir pranešimo reikalavimų srityje. Tai turėtų padėti skaitmeninius paslaugų teikėjus vertinti vienodai visoje Sąjungoje, proporcingai atsižvelgiant į rizikos, su kuria jie gali susidurti, pobūdį ir laipsnį;

(58) šia direktyva neturėtų būti draudžiama valstybėms narėms nustatyti saugumo ir pranešimo reikalavimus subjektams, kurie nėra skaitmeninių paslaugų teikėjai, kuriems taikoma ši direktyva, nedarant poveikio valstybių narių pareigoms pagal Sąjungos teisę;

(59) kompetentingos institucijos turėtų skirti deramą dėmesį neformalių ir patikimų dalijimosi informacija kanalų išsaugojimui. Viešinant incidentus, apie kuriuos pranešama kompetentingoms institucijoms, turėtų būti tinkamai subalansuojamas visuomenės interesas būti informuotai apie grėsmes, kurios gali padaryti žalos apie incidentus pranešančių esminių paslaugų operatorių ir skaitmeninių paslaugų teikėjų reputacijai ir komercinei veiklai. Įgyvendindamos pranešimo pareigas, kompetentingos institucijos ir CSIRT turėtų skirti ypač daug dėmesio poreikiui užtikrinti, kad informacija apie produkto pažeidžiamumą būtų visiškai konfidenciali iki bus paskelbtos atitinkamos saugumo priemonės;

(60) turėtų būti vykdoma skaitmeninių paslaugų teikėjų negriežta ir reaguojamoji *ex post* priežiūra, grindžiama jų teikiamų paslaugų ir atliekamų operacijų pobūdžiu. Todėl atitinkama kompetentinga institucija veiksmų turėtų imtis tik tada, kai gauna įrodymų, pavyzdžiui, iš paties skaitmeninių paslaugų teikėjo, kitos kompetentingos institucijos, įskaitant kitos valstybės narės kompetentingą instituciją, arba iš paslaugos naudotojo, kad skaitmeninių paslaugų teikėjas nesilaiko šios direktyvos reikalavimų, visų pirma po įvykusio incidento. Todėl kompetentinga institucija neturėtų turėti bendros pareigos prižiūrėti skaitmeninių paslaugų teikėjų;

(61) kompetentingos institucijos turėtų turėti būtinų priemonių savo pareigoms vykdyti, įskaitant įgaliojimus gauti pakankamai informacijos, kad būtų galima įvertinti tinklų ir informacinių sistemų saugumo lygį;

(62) incidentai gali kilti dėl nusikalstamos veikos; prie jų prevencijos, tyrimo ir baudžiamojo persekiojimo už juos prisidedama esminių paslaugų operatorių, skaitmeninių paslaugų teikėjų, kompetentingų institucijų ir teisėsaugos institucijų veiklos koordinavimu ir bendradarbiavimu. Kai įtariama, kad incidentas yra susijęs su sunkia nusikalstama veika pagal Sąjungos ar nacionalinę teisę, valstybės narės turėtų skatinti esminių paslaugų operatorius ir skaitmeninių paslaugų teikėjus atitinkamoms teisėsaugos institucijoms pranešti apie įtariamo sunkaus nusikalstamo pobūdžio incidentus. Atitinkamais atvejais pageidautina, kad įvairių valstybių narių kompetentingų institucijų ir teisėsaugos institucijų veiklos koordinavimą palengvintų Europos kovos su elektroniniu nusikalstamumu centras (EC3) ir ENISA;

(63) daugeliu atvejų dėl incidentų kyla pavojus asmens duomenų saugumui. Šiomis aplinkybėmis kompetentingos institucijos ir duomenų apsaugos institucijos turėtų bendradarbiauti ir keistis informacija visais su tuo susijusiais klausimais, kad galėtų imtis bet kokių dėl incidentų įvykusių asmens duomenų saugumo pažeidimų nagrinėjimo;

(64) jurisdikcija skaitmeninių paslaugų teikėjų atžvilgiu turėtų būti priskirta valstybei narei, kurioje yra atitinkamo skaitmeninių paslaugų teikėjo pagrindinė verslo vieta Sąjungoje, kuri iš esmės atitinka vietą, kurioje yra paslaugų teikėjo pagrindinė buveinė Sąjungoje. Verslo vieta reiškia, kad naudojantis stabiliomis struktūromis vykdoma veiksminga ir reali veikla. Teisinė tokių struktūrų forma, neatsižvelgiant į tai, ar tai filialas ar patronuojamoji bendrovė, turinti juridinio asmens statusą, šiuo požiūriu nėra lemiamas veiksnys. Šis kriterijus neturėtų

priklausyti nuo to, ar tinklų ir informacinės sistemos fiziškai yra tam tikroje vietoje; tai, kad tokios sistemos yra ir yra naudojamos, savaime nereiškia tokios pagrindinės verslo vietos ir todėl tai nelaikoma pagrindinės verslo vietos nustatymo kriterijumi;

(65) kai skaitmeninių paslaugų teikėjas, kuris nėra įsisteigęs Sąjungoje, siūlo paslaugas Sąjungoje, jis turėtų paskirti atstovą. Siekiant nustatyti, ar toks skaitmeninių paslaugų teikėjas siūlo paslaugas Sąjungoje, turėtų būti išsiaiškinta, ar akivaizdu, kad tas skaitmeninių paslaugų teikėjas planuoja siūlyti paslaugas asmenims vienoje ar daugiau valstybių narių. Vien to, kad Sąjungoje yra prieinama skaitmeninės paslaugos teikėjo ar tarpininko svetainė ar el. pašto adresas ir kiti kontaktiniai duomenys arba kad vartojama kalba, kuri paprastai vartojama trečiojoje valstybėje, kurioje yra įsisteigęs skaitmeninės paslaugos teikėjas, nepakanka siekiant įrodyti, kad esama tokio ketinimo. Vis dėlto, dėl tokių veiksnių kaip antai kalbos ar valiutos, paprastai vartojamų (naudojamų) vienoje ar daugiau valstybių narių vartojimas (naudojimas) su galimybe užsisakyti paslaugas ta kita kalba, arba Sąjungoje esančių vartotojų ar naudotojų paminėjimas gali būti aišku, kad skaitmeninių paslaugų teikėjas planuoja siūlyti paslaugas Sąjungoje. Atstovas turėtų veikti skaitmeninių paslaugų teikėjo vardu, o kompetentingos institucijos arba CSIRT turėtų turėti galimybę kreiptis į atstovą. Atstovas turėtų būti aiškiai paskirtas skaitmeninių paslaugų teikėjo rašytiniu įgaliojimu veikti jo vardu vykdant pastarojo pareigas, įskaitant pranešimą apie incidentus, pagal šią direktyvą;

(66) saugumo reikalavimų standartizavimas yra rinkos principais grindžiamas procesas. Norėdamos užtikrinti vienodą saugumo standartų taikymą, valstybės narės turėtų skatinti nurodytų standartų laikymąsi ar atitiktį jiems, kad Sąjungos lygmeniu būtų užtikrintas aukštas tinklų ir informacinių sistemų saugumo lygis. ENISA turėtų padėti valstybėms narėms teikdama konsultacijas ir gaires. Tuo tikslu galėtų būti naudinga parengti darniųjų standartų projektus; tai turėtų būti daroma laikantis Europos Parlamento ir Tarybos reglamento (ES) Nr. 1025/2012 ([1]);

(67) subjektai, kuriems netaikoma ši direktyva, gali patirti incidentų, darančių didelį poveikį jų teikiamoms paslaugoms. Kai tie subjektai mano, kad dėl viešojo intereso apie tokius įvykusius incidentus reikėtų pranešti, jie turėtų turėti teisę tai daryti savanoriškai. Kompetentinga institucija arba CSIRT turėtų tvarkyti tokius pranešimus, jei dėl tokio tvarkymo atitinkamoms valstybėms narėms neužkraunama neproporcinga arba netinkama našta;

(68) siekiant užtikrinti vienodas šios direktyvos įgyvendinimo sąlygas, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai apibrėžti procedūrinę tvarką, būtiną Bendradarbiavimo grupės veikimui užtikrinti, ir skaitmeninių paslaugų teikėjams taikytinus saugumo ir pranešimo reikalavimus. Tais įgaliojimais turėtų būti naudojamasi laikantis Europos Parlamento ir Tarybos reglamento (ES) Nr. 182/2011 ([2]). Priimdama įgyvendinimo aktus, susijusius su procedūrine tvarka, būtina Bendradarbiavimo grupės veikimui užtikrinti, Komisija turėtų kiek įmanoma labiau atsižvelgti į ENISA nuomonę;

(69) priimdama įgyvendinimo aktus, susijusius su skaitmeninių paslaugų teikėjams taikytinais saugumo ir pranešimo reikalavimais, Komisija turėtų kiek įmanoma labiau atsižvelgti į ENISA nuomonę ir konsultuotis su suinteresuotaisiais subjektais. Be to, Komisija skatinama atsižvelgti į šiuos pavyzdžius: kiek tai susiję su sistemų ir įrenginių saugumu: fizinį ir aplinkos saugumą, tiekimo saugumą, prieigos prie tinklų ir informacinių sistemų kontrolę bei tinklų ir informacinių sistemų vientisumą; kiek tai susiję su incidentų valdymu: incidentų valdymo procedūras, incidentų nustatymo pajėgumą, pranešimo apie incidentus ir ryšių palaikymą; kiek tai susiję su verslo tęstinumo valdymu: paslaugų tęstinumo strategiją ir nenumatytų atvejų planus, veiklos atkūrimo po ekstremaliųjų įvykių pajėgumus; ir kas susiję su stebėsena, auditu ir testavimu: stebėsenos ir registravimo politiką, nenumatytų atvejų planų įgyvendinimą, tinklų ir informacinių sistemų testavimą, saugumo vertinimus ir reikalavimų laikymosi stebėseną;

(70) įgyvendindama šią direktyvą Komisija prireikus turėtų veikti kartu su atitinkamais sektorių komitetais ir atitinkamomis Sąjungos lygmeniu įsteigtomis įstaigomis šios direktyvos taikymo srityse;

([1]) 2012 m. spalio 25 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1025/2012 dėl Europos standartizacijos, kuriuo iš dalies keičiamos Tarybos direktyvos 89/686/EEB ir 93/15/EEB ir Europos Parlamento ir Tarybos direktyvos 94/9/EB, 94/25/EB, 95/16/EB, 97/23/EB, 98/34/EB, 2004/22/EB, 2007/23/EB, 2009/23/EB ir 2009/105/EB ir panaikinamas Tarybos sprendimas 87/95/EEB ir Europos Parlamento ir Tarybos sprendimas Nr. 1673/2006/EB (OL L 316, 2012 11 14, p. 12).

([2]) 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).

(71) Komisija, konsultuodamasi su suinteresuotaisiais subjektais, turėtų periodiškai peržiūrėti šią direktyvą, visų pirma siekdama nustatyti, ar reikia ją keisti atsižvelgiant į kintančias visuomenines, politines, technologines ar rinkos sąlygas;

(72) dalijantis informacija apie riziką ir incidentus Bendradarbiavimo grupėje bei CSIRT tinkle ir laikantis reikalavimų pranešti apie incidentus nacionalinėms kompetentingoms institucijoms arba CSIRT, galėtų reikėti tvarkyti asmens duomenis. Tvarkant asmens duomenis turėtų būti laikomasi Europos Parlamento ir Tarybos direktyvos 95/46/EB ([1]) ir Europos Parlamento ir Tarybos reglamento (EB) Nr. 45/2001 ([2]). Taikant šią direktyvą prireikus turėtų būti taikomas Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1049/2001 ([3]);

(73) vadovaujantis Reglamento (EB) Nr. 45/2001 28 straipsnio 2 dalimi buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu, kuris pateikė nuomonę 2013 m. birželio 14 d. ([4]);

(74) kadangi šios direktyvos tikslo, t.y. užtikrinti aukštą bendrą tinklų ir informacinių sistemų saugumo lygį Sąjungoje, valstybės narės negali deramai pasiekti, o dėl siūlomo veiksmo poveikio to tikslo būtų geriau siekti Sąjungos lygiu, laikydamasi Europos Sąjungos sutarties 5 straipsnyje nustatyto subsidiarumo principo Sąjunga gali patvirtinti priemones. Pagal tame straipsnyje nustatytą proporcingumo principą šia direktyva neviršijama to, kas būtina nurodytam tikslui pasiekti;

(75) šioje direktyvoje užtikrinamos pagrindinės teisės ir laikomasi principų, pripažintų Europos Sąjungos pagrindinių teisių chartijoje, visų pirma teisė į privatų gyvenimą ir komunikacijas, teisė į asmens duomenų apsaugą, laisvė užsiimti verslu, teisė į nuosavybę, teisė į veiksmingą teisinę gynybą ir teisė būti išklausytam. Ši direktyva turėtų būti įgyvendinta atsižvelgiant į tas teises ir principus,

PRIĖMĖ ŠIĄ DIREKTYVĄ:

I SKYRIUS

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas ir taikymo sritis

1. Šioje direktyvoje nustatomos priemonės aukštam bendram tinklų ir informacinių sistemų saugumo lygiui Sąjungoje užtikrinti, kad būtų pagerintas vidaus rinkos veikimas.

2. Tuo tikslu šia direktyva:

a) visoms valstybėms narėms nustatomos pareigos priimti nacionalinę tinklų ir informacinių sistemų saugumo strategiją;

b) sukuriama Bendradarbiavimo grupė, kad būtų remiamas ir lengvinamas valstybių narių strateginis bendradarbiavimas ir keitimasis informacija, taip pat didinama jų atsakomybė ir tarpusavio pasitikėjimas;

c) sukuriamas Reagavimo į kompiuterinius saugumo incidentus tarnybų tinklas (toliau – CSIRT tinklas), kad būtų prisidedama prie valstybių narių atsakomybės ir tarpusavio pasitikėjimo didinimo ir skatinamas greitas bei veiksmingas operatyvinis bendradarbiavimas;

([1]) 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).
([2]) 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).
([3]) 2001 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1049/2001 dėl galimybės visuomenei susipažinti su Europos Parlamento, Tarybos ir Komisijos dokumentais (OL L 145, 2001 5 31, p. 43).
([4]) OL C 32, 2014 2 4, p. 19.

d) nustatomi saugumo ir pranešimo reikalavimai esminių paslaugų operatoriams ir skaitmeninių paslaugų teikėjams;

e) nustatomos valstybių narių pareigos paskirti nacionalines kompetentingas institucijas, bendruosius informacinius centrus ir CSIRT, kuriems pavedamos užduotys, susijusios su tinklų ir informacinių sistemų saugumu.

3. Šioje direktyvoje numatyti saugumo ir pranešimo reikalavimai netaikomi įmonėms, kurioms taikomi Direktyvos 2002/21/EB 13a ir 13b straipsniuose nustatyti reikalavimai, ir patikimumo užtikrinimo paslaugų teikėjams, kuriems taikomi Reglamento (ES) Nr. 910/2014 19 straipsnyje nustatyti reikalavimai.

4. Ši direktyva taikoma nedarant poveikio Tarybos direktyvai 2008/114/EB ([1]) ir Europos Parlamento ir Tarybos direktyvoms 2011/93/ES ([2]) ir 2013/40/ES ([3]).

5. Nedarant poveikio SESV 346 straipsniui, informacija, kuri yra konfidenciali pagal Sąjungos ir nacionalines taisykles, kaip antai taisykles dėl verslo konfidencialumo, turi būti keičiamasi su Komisija ir kitomis atitinkamomis institucijomis tik kai toks keitimasis yra būtinas šios direktyvos taikymui. Keičiamasi tik tokia informacija, kuri atitinka keitimosi tikslą ir yra svarbi tam tikslui pasiekti. Keičiantis tokia informacija turi būti saugomas tos informacijos konfidencialumas, ir esminių paslaugų operatorių bei skaitmeninių paslaugų teikėjų saugumo ir komerciniai interesai.

6. Šia direktyva nedaromas poveikis veiksmams, kurių valstybės narės imasi siekdamos apsaugoti savo esmines valstybines funkcijas, visų pirma užtikrinti nacionalinį saugumą, įskaitant veiksmus, skirtus informacijai, kurios atskleidimas, valstybių narių nuomone, prieštarautų gyvybiniams jų saugumo interesams, apsaugoti, taip pat palaikyti viešąją tvarką, visų pirma sudaryti sąlygas tirti ir išaiškinti nusikalstamas veikas, ir už jas patraukti baudžiamojon atsakomybėn.

7. Kai pagal konkrečiam sektoriui taikomą Sąjungos teisės aktą reikalaujama, kad esminių paslaugų operatoriai arba skaitmeninių paslaugų teikėjai užtikrintų savo tinklų ir informacinių sistemų saugumą arba praneštų apie incidentus, jei tokių reikalavimų poveikis yra bent lygiavertis šioje direktyvoje nustatytų pareigų poveikiui, taikomos tos minėto konkrečiam sektoriui taikomo Sąjungos teisės akto nuostatos.

2 straipsnis

Asmens duomenų tvarkymas

1. Asmens duomenų tvarkymas pagal šią direktyvą vykdomas laikantis Direktyvos 95/46/EB.

2. Sąjungos institucijos ir įstaigos asmens duomenis pagal šią direktyvą tvarko laikydamosi Reglamento (EB) Nr. 45/2001.

3 straipsnis

Minimalus suderinimas

Nedarant poveikio 16 straipsnio 10 daliai ir valstybių narių pareigoms pagal Sąjungos teisę, valstybės narės gali priimti ar palikti galioti nuostatas aukštesniam tinklų ir informacinių sistemų saugumo lygiui užtikrinti.

([1]) 2008 m. gruodžio 8 d. Tarybos direktyva 2008/114/EB dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo (OL L 345, 2008 12 23, p. 75).

([2]) 2011 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyva 2011/93/ES dėl kovos su seksualine prievarta prieš vaikus, jų seksualiniu išnaudojimu ir vaikų pornografija, kuria pakeičiamas Tarybos pamatinis sprendimas 2004/68/TVR (OL L 335, 2011 12 17, p. 1).

([3]) 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (OL L 218, 2013 8 14, p. 8).

4 straipsnis

Terminų apibrėžtys

Šioje direktyvoje vartojamų terminų apibrėžtys:

1) tinklų ir informacinė sistema – tai:

   a) elektroninių ryšių tinklas, kaip apibrėžta Direktyvos 2002/21/EB 2 straipsnio a punkte;

   b) bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba

   c) skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami a ir b punktuose nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais;

2) tinklų ir informacinių sistemų saugumas – tinklų ir informacinių sistemų pajėgumas tam tikru patikimumo lygiu išlikti atsparus bet kuriems veiksmams, keliantiems pavojų saugomų, perduodamų ar tvarkomų duomenų, arba atitinkamų teikiamų ar per tas tinklų ir informacines sistemas gaunamų paslaugų prieinamumui, autentiškumui, vientisumui ar konfidencialumui;

3) nacionalinė tinklų ir informacinių sistemų saugumo strategija – sistema, kurioje nustatomi strateginiai tikslai ir prioritetai dėl tinklų ir informacinių sistemų saugumo nacionaliniu lygmeniu;

4) esminių paslaugų operatorius – viešojo arba privačiojo sektoriaus subjektas, kurio rūšis yra nurodyta II priede ir kuris tenkina 5 straipsnio 2 dalyje nustatytus kriterijus;

5) skaitmeninė paslauga – paslauga, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2015/1535 ([1]) 1 straipsnio 1 dalies b punkte, kuri yra vienos iš III priede išvardytų rūšių;

6) skaitmeninių paslaugų teikėjas – juridinis asmuo, kuris teikia skaitmenines paslaugas;

7) incidentas – įvykis, turintis faktinį neigiamą poveikį tinklų ir informacinių sistemų saugumui;

8) incidentų valdymas – visos procedūros, padedančios nustatyti, ištirti bei suvaldyti incidentą ir į jį reaguoti;

9) rizika – pagrįstai nustatoma aplinkybė ar įvykis, galintis turėti neigiamą poveikį tinklų ir informacinių sistemų saugumui;

10) atstovas – Sąjungoje įsisteigęs fizinis arba juridinis asmuo, aiškiai paskirtas veikti skaitmeninių paslaugų teikėjo, kuris nėra įsisteigęs Sąjungoje, vardu ir į kurį vietoj skaitmeninių paslaugų teikėjo gali kreiptis nacionalinė kompetentinga institucija arba CSIRT dėl pagal šią direktyvą nustatytų to skaitmeninių paslaugų teikėjo pareigų;

11) standartas – standartas, kaip apibrėžta Reglamento (ES) Nr. 1025/2012 2 straipsnio 1 punkte;

12) specifikacija – techninė specifikacija, kaip apibrėžta Reglamento (ES) Nr. 1025/2012 2 straipsnio 4 punkte;

13) interneto duomenų srautų mainų taškas (IXP) – tinklo įrenginys, kuris sudaro sąlygas sujungti daugiau nei dvi nepriklausomas autonomines sistemas, visų pirma siekiant palengvinti interneto duomenų srautų mainus; IXP sujungia tik autonomines sistemas; IXP atveju nėra būtina, kad interneto duomenų srautai, perduodami tarp bet kurių naudojamų autonominių sistemų porų, būtų perduodami per bet kurią trečią autonominę sistemą; be to, jis nekeičia tokių srautų ar kitokiu būdu jų netrikdo;

14) domenų vardų sistema (DNS) – pagal hierarchiją suskirstyta vardų suteikimo sistema tinkle, kuris persiunčia domenų vardų užklausas;

([1]) 2015 m. rugsėjo 9 d. Europos Parlamento ir Tarybos direktyva (ES) 2015/1535, kuria nustatoma informacijos apie techninius reglamentus ir informacinės visuomenės paslaugų taisykles teikimo tvarka (OL L 241, 2015 9 17, p. 1).

15) DNS paslaugų teikėjas – subjektas, kuris teikia DNS paslaugas internetu;

16) aukščiausio lygio domenų vardų registras – subjektas, kuris administruoja ir vykdo interneto domenų vardų registravimą pagal konkretų aukščiausio lygio domeną (ALD);

17) elektroninė prekyvietė – skaitmeninė paslauga, kuria sudaromos sąlygos vartotojams ir (arba) komercinės veiklos subjektams, apibrėžtiems atitinkamai Europos Parlamento ir Tarybos direktyvos 2013/11/ES ([1]) 4 straipsnio 1 dalies a punkte ir b punkte, sudaryti elektroninės prekybos ar paslaugų sutartis su komercinės veiklos subjektais elektroninės prekyvietės svetainėje arba komercinės veiklos subjekto svetainėje, kurioje naudojamasi elektroninės prekyvietės teikiamomis kompiuterijos paslaugomis;

18) interneto paieškos sistema – skaitmeninė paslauga, kuria sudaromos sąlygos naudotojams vykdyti paiešką iš esmės visose svetainėse arba svetainėse konkrečia kalba, remiantis bet kurio dalyko užklausa, naudojant raktinį žodį, frazę arba kitus įvesties duomenis; šioje sistemoje pateikiamos nuorodos, kuriose gali būti su ieškomu turiniu susijusios informacijos;

19) debesijos kompiuterijos paslauga – skaitmeninė paslauga, kuri suteikia prieigą prie kintamo masto pritaikomos bendrų kompiuterijos išteklių bazės.

5 straipsnis

Esminių paslaugų operatorių identifikavimas

1. Ne vėliau kaip 2018 m. lapkričio 9 d. valstybės narės kiekviename iš II priede nurodytų sektorių ir subsektorių identifikuoja esminių paslaugų operatorius, kurie yra įsisteigę jų teritorijoje.

2. Esminių paslaugų operatorių identifikavimo kriterijai, kaip nurodyta 4 straipsnio 4 punkte, yra šie:

a) subjektas teikia paslaugą, kuri yra būtina siekiant užtikrinti ypatingos svarbos visuomeninės ir (arba) ekonominės veiklos vykdymą;

b) tos paslaugos teikimas priklauso nuo tinklų ir informacinių sistemų, ir

c) incidentas turėtų didelį trikdomąjį poveikį tos paslaugos teikimui.

3. 1 dalies tikslais kiekviena valstybė narė sudaro 2 dalies a punkte nurodytų paslaugų sąrašą.

4. 1 dalies tikslais, kai subjektas teikia 2 dalies a punkte nurodytą paslaugą dviejose ar daugiau valstybių narių, tos valstybės narės konsultuojasi tarpusavyje. Tokios konsultacijos vyksta prieš priimant sprendimą dėl identifikavimo.

5. Valstybės narės reguliariai ir ne rečiau kaip kas dvejus metus nuo 2018 m. gegužės 9 d. peržiūri ir prireikus atnaujina identifikuotų esminių paslaugų operatorių sąrašą.

6. Bendradarbiavimo grupės vaidmuo, atsižvelgiant į 11 straipsnyje nurodytas užduotis, yra padėti valstybėms narėms esminių paslaugų operatorių identifikavimo procese laikytis nuoseklaus požiūrio.

7. 23 straipsnyje nurodytos peržiūros tikslais ir ne vėliau kaip 2018 m. lapkričio 9 d., o vėliau – kas dvejus metus, valstybės narės pateikia Komisijai būtiną informaciją, kad ji galėtų įvertinti šios direktyvos įgyvendinimą, visų pirma, požiūrio, kurio laikosi valstybės narės identifikuodamos esminių paslaugų operatorius, nuoseklumą. Turi būti pateikiama bent ši informacija:

a) nacionalinės priemonės, kuriomis sudaromos sąlygos identifikuoti esminių paslaugų operatorius;

([1]) 2013 m. gegužės 21 d. Europos Parlamento ir Tarybos direktyva 2013/11/ES dėl alternatyvaus vartotojų ginčų sprendimo, kuria iš dalies keičiami Reglamentas (EB) Nr. 2006/2004 ir Direktyva 2009/22/EB (Direktyva dėl vartotojų AGS) (OL L 165, 2013 6 18, p. 63).

b) 3 dalyje nurodytų paslaugų sąrašas;

c) kiekviename II priede nurodytame sektoriuje identifikuotų esminių paslaugų operatorių skaičius ir jų svarba tam sektoriui;

d) ribos, jei jų esama, siekiant nustatyti atitinkamą tiekimo lygį atsižvelgiant į naudotojų, kurie priklauso nuo tos paslaugos, kaip nurodyta 6 straipsnio 1 dalies a punkte, skaičių arba to konkretaus esminių paslaugų operatoriaus svarbą, kaip nurodyta 6 straipsnio 1 dalies f punkte.

Siekdama prisidėti prie palyginamos informacijos teikimo, Komisija, kuo įmanoma labiau atsižvelgdama į ENISA nuomonę, gali priimti atitinkamas technines gaires dėl parametrų, taikomų šioje dalyje nurodytai informacijai.

6 straipsnis

Didelis trikdomasis poveikis

1. Nustatydamos, ar trikdomasis poveikis yra didelis, kaip nurodyta 5 straipsnio 2 dalies c punkte, valstybės narės atsižvelgia bent į šiuos tarpsektorinius veiksnius:

a) naudotojų, kurie priklauso nuo atitinkamo subjekto teikiamos paslaugos, skaičių;

b) kitų II priede nurodytų sektorių priklausomybę nuo to subjekto teikiamos paslaugos;

c) poveikį, kurį incidentai dėl savo masto ir trukmės galėtų daryti ekonominei ir visuomeninei veiklai arba viešajam saugumui;

d) to subjekto užimamą rinkos dalį;

e) geografinę teritorijos, kurią galėtų paveikti incidentas, aprėptį;

f) subjekto svarbą pakankamam paslaugos lygiui išlaikyti, atsižvelgiant į esamas tos paslaugos teikimo alternatyvas.

2. Siekdamos nustatyti, ar incidentas turėtų didelį trikdomąją poveikį, valstybės narės taip pat prireikus atsižvelgia į konkretiems sektoriams būdingus veiksnius.

II SKYRIUS

NACIONALINĖS TINKLŲ IR INFORMACINIŲ SISTEMŲ SAUGUMO SISTEMOS

7 straipsnis

Nacionalinė tinklų ir informacinių sistemų saugumo strategija

1. Kiekviena valstybė narė priima nacionalinę tinklų ir informacinių sistemų saugumo strategiją, kurioje apibrėžiami strateginiai tikslai ir tinkamos politikos bei reguliavimo priemonės aukšto lygio tinklų ir informacinių sistemų saugumui pasiekti ir išlaikyti, ir kuri apima bent II priede nurodytus sektorius ir III priede nurodytas paslaugas. Nacionalinėje tinklų ir informacinių sistemų saugumo strategijoje visų pirma nagrinėjami šie klausimai:

a) nacionalinės tinklų ir informacinių sistemų saugumo strategijos tikslai ir prioritetai;

b) valdymo sistema, skirta nacionalinės tinklų ir informacinių sistemų saugumo strategijos tikslams ir prioritetams įgyvendinti, įskaitant valdžios įstaigų ir kitų atitinkamų subjektų vaidmenis ir įsipareigojimus;

c) parengties, reagavimo ir atkūrimo priemonių, įskaitant viešojo ir privačiojo sektorių bendradarbiavimą, nustatymas;

d) švietimo, informuotumo didinimo ir mokymo programų, susijusių su nacionaline tinklų ir informacinių sistemų saugumo strategija, nurodymas;

e) mokslinių tyrimų ir plėtros planų, susijusių su nacionaline tinklų ir informacinių sistemų saugumo strategija, nurodymas;

f) rizikos vertinimo planas, skirtas rizikai nustatyti;

g) įvairių subjektų, dalyvaujančių įgyvendinant nacionalinę tinklų ir informacinių sistemų saugumo strategiją, sąrašas.

2. Valstybės narės gali prašyti ENISA padėti parengti nacionalines tinklų ir informacinių sistemų saugumo strategijas.

3. Valstybės narės pateikia Komisijai nacionalines tinklų ir informacinių sistemų saugumo strategijas per tris mėnesius nuo jų priėmimo. Tai darydamos valstybės narės gali nepranešti apie su nacionaliniu saugumu susijusius strategijos elementus.

8 straipsnis

Nacionalinės kompetentingos institucijos ir bendrasis informacinis centras

1. Kiekviena valstybė narė paskiria vieną ar daugiau nacionalinių tinklų ir informacinių sistemų saugumo kompetentingų institucijų (toliau – kompetentinga institucija), kurių veikla apima bent II priede nurodytus sektorius ir III priede nurodytas paslaugas. Valstybės narės gali paskirti šį vaidmenį esamai institucijai arba institucijoms.

2. Kompetentingos institucijos stebi šios direktyvos taikymą nacionaliniu lygmeniu.

3. Kiekviena valstybė narė paskiria nacionalinį bendrąjį tinklų ir informacinių sistemų saugumo informacinį centrą (toliau – bendrasis informacinis centras). Valstybės narės gali paskirti šį vaidmenį esamai institucijai. Kai valstybė narė paskiria tik vieną kompetentingą instituciją, ta kompetentinga institucija taip pat vykdo bendrojo informacinio centro funkcijas.

4. Bendrasis informacinis centras atlieka ryšių palaikymo funkciją, kad būtų užtikrintas tarpvalstybinis valstybių narių institucijų bendradarbiavimas ir bendradarbiavimas su kitų valstybių narių atitinkamomis institucijomis, 11 straipsnyje nurodyta Bendradarbiavimo grupe ir 12 straipsnyje nurodytu CSIRT tinklu.

5. Valstybės narės užtikrina, kad kompetentingos institucijos ir bendrieji informaciniai centrai turėtų tinkamų išteklių, kad efektyviai ir veiksmingai vykdytų jiems pavestas užduotis ir taip įgyvendintų šios direktyvos tikslus. Valstybės narės užtikrina efektyvų, veiksmingą ir saugų į Bendradarbiavimo grupę paskirtų atstovų bendradarbiavimą.

6. Kompetentingos institucijos ir bendrasis informacinis centras prireikus ir pagal nacionalinę teisę konsultuojasi ir bendradarbiauja su atitinkamomis nacionalinėmis teisėsaugos institucijomis ir nacionalinėmis duomenų apsaugos institucijomis.

7. Kiekviena valstybė narė nedelsdama praneša Komisijai apie kompetentingos institucijos ir bendrojo informacinio centro paskyrimą, jų užduotis ir visus vėlesnius jų pakeitimus. Kiekviena valstybė narė viešai paskelbia apie kompetentingos institucijos ir bendrojo informacinio centro paskyrimą. Komisija paskelbia paskirtų bendrųjų informacinių centrų sąrašą.

9 straipsnis

Reagavimo į kompiuterinius saugumo incidentus tarnybos (CSIRT)

1. Kiekviena valstybė narė paskiria vieną ar daugiau CSIRT, atitinkančią I priedo 1 punkte nustatytus reikalavimus, kurios veikla apima bent II priede nurodytus sektorius ir III priede nurodytas paslaugas, ir kuri yra atsakinga už rizikos bei incidentų valdymą vadovaujantis tiksliai apibrėžtu procesu. CSIRT gali būti įsteigta kompetentingoje institucijoje.

2. Valstybės narės užtikrina, kad CSIRT turėtų tinkamų išteklių, kad galėtų efektyviai vykdyti savo užduotis, nustatytas I priedo 2 punkte.

Valstybės narės užtikrina efektyvų, veiksmingą ir saugų jų CSIRT bendradarbiavimą 12 straipsnyje nurodytame CSIRT tinkle.

3. Valstybės narės užtikrina, kad jų CSIRT turėtų prieigą prie tinkamos, saugios ir atsparios nacionalinio lygmens ryšių ir informacinės infrastruktūros.

4. Valstybės narės informuoja Komisiją apie jų CSIRT incidentų valdymo proceso mastą ir pagrindinius elementus.

5. Valstybės narės gali paprašyti ENISA padėti kurti nacionalines CSIRT.

10 straipsnis

Bendradarbiavimas nacionaliniu lygmeniu

1. Kai tos pačios valstybės narės kompetentinga institucija, bendrasis informacinis centras ir CSIRT yra atskiri, jie bendradarbiauja, kad vykdytų šioje direktyvoje nustatytas pareigas.

2. Valstybės narės užtikrina, kad kompetentingos institucijos arba CSIRT gautų pagal šią direktyvą pateiktus pranešimus apie incidentus. Kai valstybė narė nusprendžia, kad CSIRT neturi gauti pranešimų, minėtai CSIRT, kiek tai būtina jos užduotims vykdyti, suteikiama prieiga prie duomenų apie incidentus, apie kuriuos pranešė esminių paslaugų operatoriai pagal 14 straipsnio 3 ir 5 dalis arba skaitmeninių paslaugų teikėjai pagal 16 straipsnio 3 ir 6 dalis.

3. Valstybės narės užtikrina, kad kompetentingos institucijos arba CSIRT informuotų bendruosius informacinius centrus apie pagal šią direktyvą pateiktus pranešimus apie incidentus.

Ne vėliau kaip 2018 m. rugpjūčio 9 d. ir po to kiekvienais metais bendrasis informacinis centras Bendradarbiavimo grupei pateikia suvestinę ataskaitą apie gautus pranešimus, kurioje, be kita ko, nurodomas pranešimų skaičius ir incidentų, apie kuriuos pranešta, pobūdis, taip pat veiksmai, kurių buvo imtasi pagal 14 straipsnio 3 ir 5 dalis bei 16 straipsnio 3 ir 6 dalis.

III SKYRIUS

BENDRADARBIAVIMAS

11 straipsnis

Bendradarbiavimo grupė

1. Siekiant remti ir palengvinti valstybių narių strateginį bendradarbiavimą ir keitimąsi informacija, didinti atsakomybę bei tarpusavio pasitikėjimą ir užtikrinti aukštą bendrą tinklų ir informacinių sistemų saugumo lygį Sąjungoje, įsteigiama Bendradarbiavimo grupė.

Bendradarbiavimo grupė vykdo savo užduotis remdamasi dvimetėmis darbo programomis, nurodytomis 3 dalies antroje pastraipoje.

2. Bendradarbiavimo grupę sudaro valstybių narių, Komisijos ir ENISA atstovai.

Prireikus Bendradarbiavimo grupė gali pakviesti atitinkamų suinteresuotųjų subjektų atstovų dalyvauti jos darbe.

Komisija teikia sekretoriato paslaugas.

3. Bendradarbiavimo grupė vykdo šias užduotis:

a) teikia strategines gaires dėl CSIRT tinklo, įsteigto pagal 12 straipsnį, veiklos;

b) keičiasi geriausia keitimosi informacija, susijusia su pranešimu apie incidentus, kaip nurodyta 14 straipsnio 3 ir 5 dalyse bei 16 straipsnio 3 ir 6 dalyse, srityje, praktika;

c) keičiasi valstybių narių geriausia praktika ir, bendradarbiaudama su ENISA, padeda valstybėms narėms stiprinti gebėjimus tinklų ir informacinių sistemų saugumo srityje;

d) aptaria valstybių narių pajėgumus bei parengtį ir savanoriškai vertina nacionalines tinklų ir informacinių sistemų saugumo strategijas ir CSIRT veiksmingumą, taip pat nustato geriausią praktiką;

e) keičiasi informacija ir geriausia informuotumo didinimo ir mokymo srities praktika;

f) keičiasi informacija ir geriausia praktika tinklų ir informacinių sistemų saugumo mokslinių tyrimų ir plėtros srityje;

g) prireikus keičiasi patirtimi su tinklų ir informacinių sistemų saugumu susijusiais klausimais su atitinkamomis Sąjungos institucijomis, įstaigomis, tarnybomis ir agentūromis;

h) aptaria 19 straipsnyje nurodytus standartus ir specifikacijas su atitinkamų Europos standartizacijos organizacijų atstovais;

i) renka geriausią praktiką, susijusią su rizika ir incidentais;

j) kasmet nagrinėja 8 straipsnio 8 dalies antroje pastraipoje nurodytas suvestines ataskaitas;

k) aptaria darbą, vykdomą pratybų, susijusių su tinklų ir informacinių sistemų saugumu, švietimo programų ir mokymo srityje, įskaitant ENISA atliekamą darbą;

l) padedant ENISA keičiasi geriausia praktika, susijusia su valstybių narių vykdomu esminių paslaugų operatorių identifikavimu, be kita ko, susijusiu su valstybių tarpusavio priklausomybe rizikos ir incidentų atveju;

m) aptaria pranešimų apie incidentus, kaip nurodyta 14 ir 16 straipsniuose, teikimo tvarką.

Bendradarbiavimo grupė ne vėliau kaip 2018 m. vasario 9 d., o vėliau – kas dvejus metus, parengia darbo programą dėl veiksmų, kurių reikia imtis siekiant įgyvendinti tikslus ir užduotis, kurie turi atitikti šios direktyvos tikslus.

4. 23 straipsnyje nurodytos peržiūros tikslais ir ne vėliau kaip 2018 m. rugpjūčio 9 d., o vėliau – kas pusantrų metų, Bendradarbiavimo grupė parengia ataskaitą, kurioje įvertina patirtį, įgytą vykdant strateginį bendradarbiavimą pagal šį straipsnį.

5. Komisija priima įgyvendinimo aktus, kuriais nustatoma procedūrinė tvarka, būtina Bendradarbiavimo grupės veikimui užtikrinti. Tie įgyvendinimo aktai priimami laikantis 22 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

Pirmos pastraipos taikymo tikslais Komisija pateikia pirmąjį įgyvendinimo akto projektą 22 straipsnio 1 dalyje nurodytam komitetui ne vėliau kaip 2017 m. vasario 9 d.

12 straipsnis

CSIRT tinklas

1. Siekiant prisidėti prie valstybių narių tarpusavio pasitikėjimo bei atsakomybės didinimo ir skatinti greitą bei veiksmingą operatyvinį bendradarbiavimą, įsteigiamas nacionalinių CSIRT tinklas.

2. CSIRT tinklą sudaro valstybių narių CSIRT ir ES CERT atstovai. Komisija dalyvauja CSIRT tinklo veikloje stebėtojos teisėmis. ENISA teikia sekretoriato paslaugas ir aktyviai remia CSIRT tarpusavio bendradarbiavimą.

3. CSIRT tinklas vykdo šias užduotis:

a) keičiasi informacija apie CSIRT paslaugas, operacijas ir bendradarbiavimo pajėgumus;

b) valstybės narės, kurią galėjo paveikti incidentas, CSIRT atstovo prašymu keičiasi skelbtina komercine informacija, susijusia su tuo incidentu bei susijusia rizika, ir ją aptaria; tačiau bet kurios valstybės narės CSIRT gali atsisakyti prisidėti prie tos diskusijos, jei kyla rizika, kad bus pakenkta incidento tyrimui;

c) savanoriškai keičiasi skelbtina informacija apie pavienius incidentus ir ją skelbia;

d) valstybės narės CSIRT atstovo prašymu aptaria ir, kai įmanoma, apibrėžia koordinuotus tos valstybės narės jurisdikcijai priklausančius reagavimo į incidentą, kuris buvo nustatytas, veiksmus;

e) padeda valstybėms narėms šalinti tarpvalstybinius incidentus remiantis savanoriško valstybių narių savitarpio pagalbos teikimo principu;

f) aptaria, nagrinėja ir nustato tolesnes operatyvinio bendradarbiavimo formas, be kita ko, susijusias su:

   i) rizikos ir incidentų kategorijomis,

   ii) išankstiniais įspėjimais,

   iii) savitarpio pagalba,

   iv) koordinavimo principais ir tvarka tuo atveju, kai valstybės narės reaguoja į tarpvalstybinę riziką ir incidentus;

g) informuoja Bendradarbiavimo grupę apie savo veiklą ir tolesnes operatyvinio bendradarbiavimo formas, aptartas pagal f punktą, ir prašo tuo klausimu rekomendacijų;

h) aptaria per pratybas, susijusias su tinklų ir informacinių sistemų saugumu, įskaitant per ENISA rengtas pratybas, įgytą patirtį;

i) Atskiros CSIRT prašymu aptaria tos CSIRT pajėgumus ir parengtį;

j) teikia gaires siekiant palengvinti operatyvinės praktikos konvergenciją taikant šio straipsnio nuostatas dėl operatyvinio bendradarbiavimo.

4. 23 straipsnyje nurodytos peržiūros tikslais ir ne vėliau kaip 2018 m. rugpjūčio 9 d., o vėliau – kas pusantrų metų, CSIRT tinklas parengia ataskaitą, įskaitant išvadas ir rekomendacijas, kurioje įvertina patirtį, įgytą vykdant operatyvinį bendradarbiavimą pagal šį straipsnį. Ta ataskaita taip pat pateikiama Bendradarbiavimo grupei.

5. CSIRT tinklas nustato savo darbo tvarkos taisykles.

13 straipsnis

Tarptautinis bendradarbiavimas

Pagal SESV 218 straipsnį Sąjunga gali sudaryti tarptautinius susitarimus su trečiosiomis šalimis ar tarptautinėmis organizacijomis, pagal kuriuos joms būtų leidžiama dalyvauti tam tikroje Bendradarbiavimo grupės veikloje ir toks dalyvavimas būtų organizuojamas. Tokiuose susitarimuose atsižvelgiama į poreikį užtikrinti tinkamą duomenų apsaugą.

IV SKYRIUS

ESMINIŲ PASLAUGŲ OPERATORIŲ TINKLŲ IR INFORMACINIŲ SISTEMŲ SAUGUMAS

14 straipsnis

Saugumo reikalavimai ir pranešimas apie incidentus

1. Valstybės narės užtikrina, kad esminių paslaugų operatoriai imtųsi tinkamų ir proporcingų techninių ir organizacinių priemonių, kad galėtų valdyti riziką, kylančią tinklų ir informacinių sistemų, kuriais jie naudojasi vykdydami savo veiklą, saugumui. Remiantis naujausiais technikos laimėjimais, tomis priemonėmis turi būti užtikrinamas toks tinklų ir informacinių sistemų saugumo lygis, kuris atitinka atsiradusią riziką.

2. Valstybės narės užtikrina, kad esminių paslaugų operatoriai imtųsi tinkamų priemonių, kad būtų išvengta incidentų, paveikiančių tinklų ir informacinių sistemų, naudojamų tokių esminių paslaugų teikimui, saugumą, poveikio ir jis būtų kuo labiau sumažintas, siekiant užtikrinti tų paslaugų tęstinumą.

3. Valstybės narės užtikrina, kad esminių paslaugų operatoriai be nepagrįsto delsimo praneštų kompetentingai institucijai arba CSIRT apie incidentus, kurie turi didelį poveikį jų teikiamų esminių paslaugų tęstinumui. Pranešimuose pateikiama informacija, kuria remdamasi kompetentinga institucija arba CSIRT galėtų nustatyti tarpvalstybinį incidento poveikį. Pranešančiajai šaliai dėl to netenka didesnė atsakomybė.

4. Siekiant nustatyti incidento poveikio mastą, visų pirma atsižvelgiama į šiuos parametrus:

a) naudotojų, kuriuos paveikė esminės paslaugos sutrikdymas, skaičių;

b) incidento trukmę;

c) geografinę teritorijos, kurią paveikė incidentas, aprėptį.

5. Remdamasi esminių paslaugų operatoriaus pranešime pateikta informacija, kompetentinga institucija arba CSIRT informuoja kitą (-as) paveiktą (-as) valstybę (-es) narę (-es), ar incidentas daro didelį poveikį esminių paslaugų tęstinumui toje valstybėje narėje. Tai darydama kompetentinga institucija arba CSIRT, laikydamosi Sąjungos teisės arba Sąjungos teisę atitinkančių nacionalinės teisės aktų, saugo esminių paslaugų operatoriaus saugumo ir komercinius interesus, taip pat jo pranešime pateiktos informacijos konfidencialumą.

Atsižvelgdamos į aplinkybes, kompetentinga institucija arba CSIRT pranešančiajam esminių paslaugų operatoriui pateikia atitinkamą informaciją apie tolesnę veiklą, susijusią su jo pranešimu, kaip antai informaciją, kuria remiantis incidentas būtų veiksmingai valdomas.

Kompetentingos institucijos arba CSIRT prašymu bendrasis informacinis centras perduoda pirmoje pastraipoje nurodytus pranešimus kitų paveiktų valstybių narių bendriesiems informaciniams centrams.

6. Pasikonsultavusi su pranešančiuoju esminių paslaugų operatoriumi, kompetentinga institucija arba CSIRT gali informuoti visuomenę apie pavienius incidentus, jei būtina informuoti visuomenę siekiant išvengti incidento arba valdyti vykstantį incidentą.

7. Kompetentingos institucijos, veikdamos kartu su Bendradarbiavimo grupe, gali parengti ir priimti gaires dėl aplinkybių, kuriomis esminių paslaugų operatoriai privalo pranešti apie incidentus, įskaitant apie parametrus, pagal kuriuos būtų nustatytas incidento poveikio mastas, kaip nurodyta 4 dalyje.

15 straipsnis

Įgyvendinimas ir vykdymo užtikrinimas

1. Valstybės narės užtikrina, kad kompetentingos institucijos turėtų reikiamus įgaliojimus ir priemones įvertinti, ar esminių paslaugų operatoriai vykdo savo pareigas pagal 14 straipsnį, ir kokį poveikį tai daro tinklų ir informacinių sistemų saugumui.

2. Valstybės narės užtikrina, kad kompetentingos institucijos turėtų įgaliojimus ir priemones reikalauti, kad esminių paslaugų operatoriai pateiktų:

a) informaciją (įskaitant dokumentus apie saugumo politiką), kuri yra būtina norint įvertinti jų tinklų ir informacinių sistemų saugumą;

b) įrodymus, kad saugumo politika veiksmingai įgyvendinama, kaip antai, kompetentingos institucijos ar kvalifikuoto auditoriaus atlikto saugumo audito rezultatus, ir pastaruoju atveju jo rezultatus, įskaitant pagrindinius įrodymus, pateiktų kompetentingai institucijai.

Prašydama tokios informacijos ar įrodymų, kompetentinga institucija nurodo prašymo tikslą ir kokios informacijos prašoma.

3. Įvertinusi 2 dalyje nurodytą informaciją arba saugumo auditų rezultatus, kompetentinga institucija gali pateikti privalomus nurodymus esminių paslaugų operatoriams ištaisyti nustatytus trūkumus.

4. Kompetentinga institucija, nagrinėdama incidentus, dėl kurių pažeidžiamas asmens duomenų saugumas, glaudžiai bendradarbiauja su duomenų apsaugos institucijomis.

V SKYRIUS

SKAITMENINIŲ PASLAUGŲ TEIKĖJŲ TINKLŲ IR INFORMACINIŲ SISTEMŲ SAUGUMAS

16 straipsnis

Saugumo reikalavimai ir pranešimas apie incidentus

1. Valstybės narės užtikrina, kad skaitmeninių paslaugų teikėjai nustatytų tinkamas ir proporcingas technines ir organizacines priemones ir jų imtųsi, kad galėtų valdyti riziką, kylančią tinklų ir informacinių sistemų, kuriais jie naudojasi teikdami III priede nurodytas paslaugas Sąjungoje, saugumui. Remiantis naujausiais technikos laimėjimais, tomis priemonėmis užtikrinamas toks tinklų ir informacinių sistemų saugumo lygis, kuris atitinka atsiradusią riziką, ir atsižvelgiama į šiuos elementus:

a) sistemų ir įrenginių saugumą;

b) incidentų valdymą;

c) veiklos tęstinumo valdymą;

d) stebėseną, auditą ir bandymus;

e) atitiktį tarptautiniams standartams.

2. Valstybės narės užtikrina, kad skaitmeninių paslaugų teikėjai imtųsi priemonių, kad būtų išvengta incidentų, darančių poveikį jų tinklų ir informacinių sistemų saugumui, poveikio III priede nurodytoms Sąjungoje teikiamoms paslaugoms ir jis būtų kuo labiau sumažintas, siekiant užtikrinti tų paslaugų tęstinumą.

3. Valstybės narės užtikrina, kad skaitmeninių paslaugų teikėjai be nepagrįsto delsimo praneštų kompetentingai institucijai arba CSIRT apie incidentą, kuris turi didelį poveikį III priede nurodytos paslaugos, kurią jie teikia Sąjungoje, teikimui. Pranešimuose pateikiama informacija, kuria remdamasi kompetentinga institucija arba CSIRT galėtų nustatyti tarpvalstybinio poveikio mastą. Pranešančiajai šaliai dėl to netenka didesnė atsakomybė.

4. Siekiant nustatyti, ar incidentas sukelia didelį poveikį, visų pirma atsižvelgiama į šiuos parametrus:

a) naudotojų, kuriuos paveikė incidentas, skaičių, visų pirma naudotojų, kurių pačių paslaugų teikimas priklauso nuo tos paslaugos;

b) incidento trukmę;

c) geografinę teritorijos, kurią paveikė incidentas, aprėptį;

d) paslaugos veikimo sutrikdymo mastą;

e) poveikio ekonominei ir visuomeninei veiklai mastą.

Pareiga pranešti apie incidentą taikoma tik tuo atveju, kai skaitmeninių paslaugų teikėjas gali naudotis informacija, kuri reikalinga įvertinti incidento poveikį atsižvelgiant į pirmoje pastraipoje nurodytus parametrus.

5. Kai esminių paslaugų teikėjas priklauso nuo trečiosios šalies skaitmeninių paslaugų teikėjo teikdamas paslaugą, kuri yra būtina siekiant užtikrinti ypatingos svarbos visuomeninės ir ekonominės veiklos vykdymą, tas operatorius praneša apie bet kokį didelį poveikį esminių paslaugų tęstinumui, kurį padarė incidentas, paveikęs skaitmeninių paslaugų teikėją.

6. Atitinkamais atvejais, ir visų pirma jei 3 dalyje nurodytas incidentas susijęs su dviem ar daugiau valstybių narių, kompetentinga institucija arba CSIRT informuoja kitas paveiktas valstybes nares. Tai darydamos kompetentingos institucijos, CSIRT ir bendrieji informaciniai centrai, laikydamiesi Sąjungos teisės arba Sąjungos teisę atitinkančių nacionalinės teisės aktų, saugo skaitmeninių paslaugų teikėjo saugumo ir komercinius interesus, taip pat pateiktos informacijos konfidencialumą.

7. Pasikonsultavusi su atitinkamu skaitmeninių paslaugų teikėju, kompetentinga institucija arba CSIRT ir, prireikus, kitų atitinkamų valstybių narių institucijos arba CSIRT gali informuoti visuomenę apie pavienius incidentus arba reikalauti, kad tai padarytų skaitmeninių paslaugų teikėjas, jei būtina informuoti visuomenę siekiant išvengti incidento ar valdyti vykstantį incidentą arba jei incidento atskleidimas kitais atvejais atitinka viešąjį interesą.

8. Komisija priima įgyvendinimo aktus, kuriais toliau apibrėžiami šio straipsnio 1 dalyje nurodyti elementai ir 4 dalyje išvardyti parametrai. Tie įgyvendinimo aktai priimami laikantis 22 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros ne vėliau kaip 2017 m. rugpjūčio 9 d.

9. Komisija gali priimti įgyvendinimo aktus, kuriais nustato pranešimo reikalavimams taikytinus formatus ir procedūras. Tie įgyvendinimo aktai priimami laikantis 22 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

10. Nedarant poveikio 1 straipsnio 6 daliai, valstybės narės nenustato jokių papildomų saugumo ar pranešimo reikalavimų skaitmeninių paslaugų teikėjams.

11. V skyrius netaikomas mikroįmonėms ir mažosioms įmonėms, kaip apibrėžta Komisijos rekomendacijoje 2003/361/EB ([1]).

([1]) 2003 m. gegužės 6 d. Komisijos rekomendacija 2003/361/EB dėl mikroįmonių, mažųjų ir vidutinių įmonių apibrėžimo (OL L 124, 2003 5 20, p. 36).

17 straipsnis

Įgyvendinimas ir vykdymo užtikrinimas

1. Valstybės narės užtikrina, kad kompetentingos institucijos imtųsi veiksmų, jei būtina, vykdydamos *ex post* priežiūros priemones, kai gauna įrodymų, kad skaitmeninių paslaugų teikėjas neatitinka 16 straipsnyje nustatytų reikalavimų. Tokius įrodymus gali pateikti kitos valstybės narės, kurioje paslauga teikiama, kompetentinga institucija.

2. 1 dalies taikymo tikslais kompetentingos institucijos turi būtinus įgaliojimus ir priemones reikalauti, kad skaitmeninių paslaugų teikėjai:

a) pateiktų informaciją (įskaitant saugumo politikos dokumentus), kuri reikalinga jų tinklų ir informacinių sistemų saugumui įvertinti;

b) ištaisytų 16 straipsnyje nustatytų reikalavimų vykdymo pažeidimus.

3. Jei skaitmeninių paslaugų teikėjo pagrindinė verslo vieta arba atstovas yra valstybėje narėje, bet jo tinklų ir informacinės sistemos yra vienoje ar daugiau kitų valstybių narių, valstybės narės, kurioje yra pagrindinė verslo vieta arba atstovas, kompetentinga institucija ir tų kitų valstybių narių kompetentingos institucijos prireikus bendradarbiauja ir padeda viena kitai. Tokia pagalba ir bendradarbiavimas gali apimti keitimąsi informacija tarp atitinkamų kompetentingų institucijų ir prašymus vykdyti 2 dalyje nurodytas priežiūros priemones.

18 straipsnis

Jurisdikcija ir teritoriškumas

1. Šios direktyvos tikslais laikoma, kad skaitmeninių paslaugų teikėjas priklauso valstybės narės, kurioje yra jo pagrindinė verslo vieta, jurisdikcijai. Laikoma, kad skaitmeninių paslaugų teikėjo pagrindinė verslo vieta yra valstybėje narėje, kai jo pagrindinė buveinė yra toje valstybėje narėje.

2. Skaitmeninių paslaugų teikėjas, kuris nėra įsisteigęs Sąjungoje, bet teikia III priede nurodytas paslaugas Sąjungoje, paskiria atstovą Sąjungoje. Atstovas turi būti įsisteigęs vienoje iš tų valstybių narių, kuriose teikiamos paslaugos. Laikoma, kad skaitmeninių paslaugų teikėjas priklauso valstybės narės, kurioje yra įsisteigęs jo atstovas, jurisdikcijai.

3. Skaitmeninių paslaugų teikėjo atstovo skyrimas nedaro poveikio teisiniams veiksmams, kurie gali būti inicijuoti prieš patį skaitmeninių paslaugų teikėją.

VI SKYRIUS

STANDARTIZACIJA IR SAVANORIŠKAS PRANEŠIMAS

19 straipsnis

Standartizacija

1. Siekdamos skatinti vienodą 14 straipsnio 1 ir 2 dalių bei 16 straipsnio 1 ir 2 dalių įgyvendinimą, valstybės narės, nereikalaudamos taikyti kokios nors konkrečios rūšies technologijos ir nesuteikdamos jai pirmenybės, skatina naudotis europiniais ar tarptautiniu mastu pripažintais standartais ir specifikacijomis, kurie yra svarbūs tinklų ir informacinių sistemų saugumui.

2. ENISA, bendradarbiaudama su valstybėmis narėmis, parengia rekomendacijas ir gaires dėl techninių sričių, kurios turi būti apsvarstytos 1 dalies atžvilgiu, taip pat dėl jau galiojančių standartų, be kita ko, valstybių narių nacionalinių standartų, kuriuose būtų numatyta įtraukti tas sritis.

20 straipsnis

Savanoriškas pranešimas

1. Nedarant poveikio 3 straipsniui, subjektai, kurie nebuvo identifikuoti kaip esminių paslaugų operatoriai ir kurie nėra skaitmeninių paslaugų teikėjai, gali savanoriškai pranešti apie incidentus, kurie daro didelį poveikį jų teikiamų paslaugų tęstinumui.

2. Tvarkydamos tokius pranešimus valstybės narės veikia pagal 14 straipsnyje nustatytą procedūrą. Valstybės narės gali teikti pirmenybę privalomų pranešimų tvarkymui, lyginant su savanoriškais pranešimais. Savanoriški pranešimai tvarkomi tik tuo atveju, jei dėl tokio tvarkymo atitinkamoms valstybėms narėms neužkraunama neproporcinga arba netinkama našta.

Dėl savanoriško pranešimo pranešančiajam subjektui nenustatoma jokių pareigų, kurios jam nebūtų buvusios nustatytos, jei jis nebūtų pateikęs to pranešimo.

VII SKYRIUS

BAIGIAMOSIOS NUOSTATOS

21 straipsnis

Sankcijos

Valstybės narės nustato sankcijų, taikomų pažeidus pagal šią direktyvą priimtas nacionalines nuostatas, taisykles ir būtinų priemonių užtikrinti, kad šios sankcijos būtų įgyvendinamos. Numatytos sankcijos turi būti veiksmingos, proporcingos ir atgrasomos. Valstybės narės praneša apie tas taisykles ir tas priemones Komisijai ne vėliau kaip 2018 m. gegužės 9 d. ir jai praneša apie visus vėlesnius joms įtakos turinčius pakeitimus.

22 straipsnis

Komiteto procedūra

1. Komisijai padeda Tinklų ir informacinių sistemų saugumo 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.

23 straipsnis

Peržiūra

1. Ne vėliau kaip 2019 m. gegužės 9 d. Komisija pateikia Europos Parlamentui ir Tarybai ataskaitą, kurioje įvertina požiūrio, kurio laikosi valstybės narės identifikuodamos esminių paslaugų operatorius, nuoseklumą.

2. Komisija periodiškai peržiūri šios direktyvos taikymą ir teikia ataskaitą Europos Parlamentui ir Tarybai. Šiuo tikslu ir siekiant tolesnės pažangos vykdant strateginį ir operatyvinį bendradarbiavimą, Komisija atsižvelgia į Bendradarbiavimo grupės ir CSIRT tinklo ataskaitas apie patirtį, įgytą strateginiu ir operatyviniu lygmeniu. Atlikdama peržiūrą Komisija taip pat įvertina II ir III prieduose pateiktus sąrašus ir esminių paslaugų operatorių bei paslaugų II priede nurodytuose sektoriuose identifikavimo nuoseklumą. Pirmoji ataskaita pateikiama ne vėliau kaip 2021 m. gegužės 9 d.

24 straipsnis

Pereinamojo laikotarpio priemonės

1. Nedarant poveikio 25 straipsniui ir siekiant suteikti valstybėms narėms papildomų tinkamo bendradarbiavimo galimybių direktyvos perkėlimo į nacionalinę teisę laikotarpiu, Bendradarbiavimo grupė ir CSIRT tinklas pradeda atlikti užduotis, nustatytas atitinkamai 11 straipsnio 3 dalyje ir 12 straipsnio 3 dalyje, ne vėliau kaip 2017 m. vasario 9 d.

2. Laikotarpiu nuo 2017 m. vasario 9 d. iki 2018 m. lapkričio 9 d. bei siekiant remti valstybes nares, kad jos esminių paslaugų operatorių identifikavimo procese laikytųsi nuoseklaus požiūrio, Bendradarbiavimo grupė aptaria nacionalinių priemonių, kuriomis sudaromos sąlygos identifikuoti esminių paslaugų operatorius konkrečiame sektoriuje remiantis 5 ir 6 straipsniuose nustatytais kriterijais, taikymo procesą, turinį ir rūšį. Bendradarbiavimo grupė, valstybės narės prašymu, taip pat aptaria konkrečius tos valstybės narės nacionalinių priemonių projektus, kuriais sudaromos sąlygos identifikuoti esminių paslaugų operatorius konkrečiame sektoriuje remiantis 5 ir 6 straipsniuose nustatytais kriterijais.

3. Valstybės narės ne vėliau kaip 2017 m. vasario 9 d. ir šio straipsnio tikslais užtikrina, kad būtų tinkamai atstovaujama Bendradarbiavimo grupėje ir CSIRT tinkle.

25 straipsnis

Perkėlimas į nacionalinę teisę

1. Valstybės narės ne vėliau kaip 2018 m. gegužės 9 d. priima ir paskelbia įstatymus ir kitus teisės aktus, būtinus, kad būtų laikomasi šios direktyvos. Apie tai jos nedelsdamos praneša Komisijai.

Tas nuostatas jos taiko nuo 2018 m. gegužės 10 d.

Valstybės narės, priimdamos tas nuostatas, daro jose nuorodą į šią direktyvą arba tokia nuoroda daroma jas oficialiai skelbiant. Tokios nuorodos darymo tvarką nustato valstybės narės.

2. Valstybės narės pateikia Komisijai šios direktyvos taikymo srityje priimtų nacionalinės teisės aktų pagrindinių nuostatų tekstus.

26 straipsnis

Įsigaliojimas

Ši direktyva įsigalioja dvidešimtą dieną po jos paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

27 straipsnis

Adresatai

Ši direktyva skirta valstybėms narėms.

Priimta Strasbūre 2016 m. liepos 6 d.

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkas	*Pirmininkas*
M. SCHULZ	I. KORČOK

I PRIEDAS

REAGAVIMO Į KOMPIUTERINIUS SAUGUMO INCIDENTUS TARNYBOMS (CSIRT) KELIAMI REIKALAVIMAI IR JŲ UŽDUOTYS

CSIRT keliami reikalavimai ir jų užduotys yra tinkamai ir aiškiai apibrėžti ir grindžiami nacionaline politika ir (arba) taisyklėmis. Juos sudaro:

1) CSIRT keliami reikalavimai

   a) CSIRT užtikrina, kad jų ryšio paslaugos būtų lengvai prieinamos išvengiant kritinių funkcionavimo trikties taškų, taip pat nustato keletą būdų, kaip bet kuriuo metu susisiekti su jomis ir kitais subjektais. Be to, ryšio kanalai yra aiškiai apibrėžti ir gerai žinomi klientams ir bendradarbiavimo partneriams.

   b) CSIRT biurai ir pagalbinės informacinės sistemos veikia saugiose vietose.

   c) Veiklos tęstinumas:

      i) CSIRT aprūpinamos tinkama prašymų valdymo ir nukreipimo sistema, siekiant palengvinti perdavimą;

      ii) CSIRT turi pakankamai darbuotojų, kad būtų užtikrintas pasiekiamumas bet kuriuo metu;

      iii) CSIRT turi infrastruktūrą, kurios tęstinumas yra užtikrintas. Tuo tikslu sukuriamos rezervinių komponentų sistemos ir atsarginės darbo patalpos.

   d) CSIRT, kai jos to pageidauja, turi galimybę dalyvauti tarptautiniuose bendradarbiavimo tinkluose.

2) CSIRT užduotys

   a) CSIRT užduotys yra bent šios:

      i) stebėti incidentus nacionaliniu lygmeniu;

      ii) teikti su įvairia rizika ir incidentais susijusius išankstinius įspėjimus, perspėjimus, skelbimus ir skleisti apie juos informaciją atitinkamiems suinteresuotiesiems subjektams;

      iii) reaguoti į incidentus;

      iv) užtikrinti operatyvią rizikos bei incidentų analizę ir informuotumą apie padėtį;

      v) dalyvauti CSIRT tinkle.

   b) CSIRT užmezga bendradarbiavimo santykius su privačiuoju sektoriumi.

   c) Siekiant palengvinti bendradarbiavimą, CSIRT skatina priimti ir naudoti bendrus ar standartizuotus metodus dėl:

      i) incidentų ir rizikos valdymo procedūrų;

      ii) incidentų, rizikos ir informacijos klasifikavimo sistemų.

II PRIEDAS

SUBJEKTŲ RŪŠYS 4 STRAIPSNIO 4 PUNKTO TAIKYMO TIKSLAIS

Sektorius	Subsektorius	Subjekto rūšis
1. Energetika	a) Elektros energija	— Elektros energijos įmonės, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2009/72/EB [1] 2 straipsnio 35 punkte, vykdanti „tiekimo“ funkciją, kaip apibrėžta tos direktyvos 2 straipsnio 19 punkte
		— Skirstymo sistemų operatoriai, kaip apibrėžta Direktyvos 2009/72/EB 2 straipsnio 6 punkte
		— Perdavimo sistemų operatoriai, kaip apibrėžta Direktyvos 2009/72/EB 2 straipsnio 4 punkte
	b) Nafta	— Naftotiekių operatoriai
		— Naftos gamybos, perdirbimo ir apdorojimo įrenginių, laikymo ir perdavimo operatoriai
	c) Dujos	— Tiekimo įmonės, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2009/73/EB [2] 2 straipsnio 8 punkte
		— Skirstymo sistemų operatoriai, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 6 punkte
		— Perdavimo sistemų operatoriai, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 4 punkte
		— Laikymo sistemų operatoriai, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 10 punkte
		— SGD sistemos operatoriai, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 12 punkte
		— Gamtinių dujų įmonės, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 1 punkte
		— Gamtinių dujų perdirbimo ir apdorojimo įrenginių operatoriai
2. Transportas	a) Oro transportas	— Oro vežėjai, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (EB) Nr. 300/2008 [3] 3 straipsnio 4 punkte
		— Oro uosto valdymo organai, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2009/12/EB [4] 2 straipsnio 2 punkte, oro uostai, kaip apibrėžta tos direktyvos 2 straipsnio 1 punkte, įskaitant pagrindinius oro uostus, nurodytus Europos Parlamento ir Tarybos reglamento (ES) Nr. 1315/2013 [5] II priedo 2 skirsnyje, ir subjektai, eksploatuojantys oro uostuose esančius pagalbinius įrenginius

Sektorius	Subsektorius	Subjekto rūšis
		— Skrydžių valdymo operatoriai, teikiantys skrydžių valdymo (ATC) paslaugas, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (EB) Nr. 549/2004 ([6]) 2 straipsnio 1 punkte
	b) Geležinkelių transportas	— Infrastruktūros valdytojai, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2012/34/ES ([7]) 3 straipsnio 2 punkte
		— Geležinkelio įmonės, kaip apibrėžta Direktyvos 2012/34/ES 3 straipsnio 1 punkte, įskaitant paslaugų įrenginių operatorius, kaip apibrėžta Direktyvos 2012/34/ES 3 straipsnio 12 punkte
	c) Vandens transportas	— Vidaus vandenų, jūrų ir priekrantės keleivinio ir krovininio vandens transporto bendrovės, kaip apibrėžta jūrų transporto atžvilgiu Europos Parlamento ir Tarybos reglamento (EB) Nr. 725/2004 ([8]) I priede, neįskaitant tų bendrovių naudojamų atskirų laivų
		— Uostų, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2005/65/EB ([9]) 3 straipsnio 1 punkte, įskaitant jų uosto įrenginius, kaip apibrėžta Reglamento (EB) Nr. 725/2004 2 straipsnio 11 punkte, direkcijos ir subjektai, eksploatuojantys uostuose esančias įmones ir įrenginius
		— Laivų eismo tarnybų, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2002/59/EB ([10]) 3 straipsnio o punkte, operatoriai
	d) Kelių transportas	— Kelių direkcijos, kaip apibrėžta Komisijos deleguotojo reglamento (ES) Nr. 2015/962 ([11]) 2 straipsnio 12 punkte, atsakingos už eismo valdymo kontrolę
		— Intelektinių transporto sistemų, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2010/40/ES ([12]) 4 straipsnio 1 punkte, operatoriai
3. Bankininkystė		Kredito įstaigos, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) Nr. 575/2013 ([13]) 4 straipsnio 1 punkte
4. Finansų rinkų infrastruktūros objektai		— Prekybos vietų, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2014/65/ES ([14]) 4 straipsnio 24 punkte, operatoriai
		— Pagrindinės sandorio šalys (PSŠ), kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) Nr. 648/2012 ([15]) 2 straipsnio 1 punkte
5. Sveikatos priežiūros sektorius	Sveikatos priežiūros vietos (įskaitant ligonines ir privačias klinikas)	Sveikatos priežiūros paslaugų teikėjai, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2011/24/ES ([16]) 3 straipsnio g punkte

Sektorius	Subsektorius	Subjekto rūšis
6. Geriamo vandens tiekimas ir paskirstymas		Žmonėms vartoti skirto vandens, kaip apibrėžta Tarybos direktyvos 98/83/EB ([17]) 2 straipsnio 1 punkto a papunktyje, tiekėjai ir skirstytojai, bet neįskaitant skirstytojų, kurių atveju žmonėms vartoti skirto vandens skirstymas yra tik dalis jų bendrosios veiklos, susijusios su kitų produktų ir prekių platinimu, kuris nėra laikomas esmine paslauga
7. Skaitmeninė infrastruktūra		— IXP
		— DNS paslaugų teikėjai
		— ALD vardų registrai

([1]) 2009 m. liepos 13 d. Europos Parlamento ir Tarybos direktyva 2009/72/EB dėl elektros energijos vidaus rinkos bendrųjų taisyklių, panaikinanti Direktyvą 2003/54/EB (OL L 211, 2009 8 14, p. 55).
([2]) 2009 m. liepos 13 d. Europos Parlamento ir Tarybos direktyva 2009/73/EB dėl gamtinių dujų vidaus rinkos bendrųjų taisyklių, panaikinanti Direktyvą 2003/55/EB (OL L 211, 2009 8 14, p. 94).
([3]) 2008 m. kovo 11 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 300/2008 dėl civilinės aviacijos saugumo bendrųjų taisyklių ir panaikinantis Reglamentą (EB) Nr. 2320/2002 (OL L 97, 2008 4 9, p. 72).
([4]) 2009 m. kovo 11 d. Europos Parlamento ir Tarybos direktyva 2009/12/EB dėl oro uostų mokesčių (OL L 70, 2009 3 14, p. 11).
([5]) 2013 m. gruodžio 11 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1315/2013 dėl Sąjungos transeuropinio transporto tinklo plėtros gairių, kuriuo panaikinamas Sprendimas Nr. 661/2010/ES (OL L 348, 2013 12 20, p. 1).
([6]) 2004 m. kovo 10 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 549/2004, nustatantis bendro Europos dangaus sukūrimo pagrindą (pagrindų reglamentas) (OL L 96, 2004 3 31, p. 1).
([7]) 2012 m. lapkričio 21 d. Europos Parlamento ir Tarybos direktyva 2012/34/ES, kuria sukuriama bendra Europos geležinkelių erdvė (OL L 343, 2012 12 14, p. 32).
([8]) 2004 m. kovo 31 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 725/2004 dėl laivų ir uostų įrenginių apsaugos stiprinimo (OL L 129, 2004 4 29, p. 6).
([9]) 2005 m. spalio 26 d. Europos Parlamento ir Tarybos direktyva 2005/65/EB dėl uostų apsaugos stiprinimo (OL L 310, 2005 11 25, p. 28).
([10]) 2002 m. birželio 27 d. Europos Parlamento ir Tarybos direktyva 2002/59/EB, įdiegianti Bendrijos laivų eismo stebėsenos ir informacijos sistemą ir panaikinanti Tarybos direktyvą 93/75/EEB (OL L 208, 2002 8 5, p. 10).
([11]) 2014 m. gruodžio 18 d. Komisijos deleguotasis reglamentas (ES) Nr. 2015/962, kuriuo papildomos Europos Parlamento ir Tarybos direktyvos 2010/40/ES nuostatos, susijusios su visoje Europos Sąjungoje teikiamomis tikralaikės eismo informacijos paslaugomis (OL L 157, 2015 6 23, p. 21).
([12]) 2010 m. liepos 7 d. Europos Parlamento ir Tarybos direktyva 2010/40/ES dėl kelių transporto ir jo sąsajų su kitų rūšių transportu srities intelektinių transporto sistemų diegimo sistemos (OL L 207, 2010 8 6, p. 1).
([13]) 2013 m. birželio 26 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 575/2013 dėl prudencinių reikalavimų kredito įstaigoms ir investicinėms įmonėms ir kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 648/2012 (OL L 176, 2013 6 27, p. 1).
([14]) 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos direktyva 2014/65/ES dėl finansinių priemonių rinkų, kuria iš dalies keičiamos Direktyva 2002/92/EB ir Direktyva 2011/61/ES (OL L 173, 2014 6 12, p. 349).
([15]) 2012 m. liepos 4 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 648/2012 dėl ne biržos išvestinių finansinių priemonių, pagrindinių sandorio šalių ir sandorių duomenų saugyklų (OL L 201, 2012 7 27, p. 1).
([16]) 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).
([17]) 1998 m. lapkričio 3 d. Tarybos direktyva 98/83/EB dėl žmonėms vartoti skirto vandens kokybės (OL L 330, 1998 12 5, p. 32).

III PRIEDAS

SKAITMENINIŲ PASLAUGŲ RŪŠYS 4 STRAIPSNIO 5 PUNKTO TAIKYMO TIKSLAIS

1. Elektroninė prekyvietė
2. Interneto paieškos sistema
3. Debesijos kompiuterijos paslauga

ISSN 1977-0723 (elektroninis leidimas)
ISSN 1725-5120 (popierinis leidimas)

Europos Sąjungos leidinių biuras
2985 Liuksemburgas
LIUKSEMBURGAS

LT