DIREKTYVOS

EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA (ES) 2022/2555

2022 m. gruodžio 14 d.

dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva)

(Tekstas svarbus EEE)

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 Centrinio Banko nuomonę ([1]),

atsižvelgdami į Europos ekonomikos ir socialinių reikalų komiteto nuomonę ([2]),

pasikonsultavę su Regionų komitetu,

laikydamiesi įprastos teisėkūros procedūros ([3]),

kadangi:

(1) Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 ([4]) buvo siekiama sukurti kibernetinio saugumo pajėgumus visoje Sąjungoje, sumažinti grėsmes tinklų ir informacinėms sistemoms, kurios naudojamos teikiant esmines paslaugas pagrindiniuose sektoriuose, ir užtikrinti tokių paslaugų nuolatinį teikimą įvykus incidentams, taip prisidedant prie Sąjungos saugumo ir veiksmingo jos ekonomikos ir visuomenės veikimo;

(2) nuo Direktyvos (ES) 2016/1148 įsigaliojimo padaryta didelė pažanga didinant Sąjungos kibernetinio atsparumo lygį. Atlikus direktyvos peržiūrą, paaiškėjo, kad ji tapo institucinio ir reguliavimo požiūrio į kibernetinį saugumą Sąjungoje paskata ir sudarė sąlygas reikšmingam mąstysenos pokyčiui. Direktyva padėjo galutinai sukurti nacionalines tinklų ir informacinių sistemų saugumo sistemas parengiant nacionalines tinklų ir informacinių sistemų saugumo strategijas, nustatant nacionalinius pajėgumus ir įgyvendinant reguliavimo priemones, taikomas esminiams infrastruktūros objektams ir kiekvienos valstybės narės identifikuotiems subjektams. Direktyva (ES) 2016/1148 taip pat prisidėta prie bendradarbiavimo Sąjungos lygmeniu įsteigus Bendradarbiavimo grupę ir sukuriant nacionalinių reagavimo į kompiuterinius saugumo incidentus tarnybų tinklą. Nepaisant tų laimėjimų, atlikus Direktyvos (ES) 2016/1148 peržiūrą paaiškėjo jos trūkumai, trukdantys veiksmingai spręsti dabartines ir naujas kibernetinio saugumo problemas;

(3) tinklų ir informacinės sistemos dėl sparčios skaitmeninės transformacijos ir visuomenės tarpusavio junglumo, įskaitant tarpvalstybinius mainus, tapo pagrindiniu kasdienio gyvenimo aspektu. Dėl tokių pokyčių kibernetinių grėsmių padėtis tapo sudėtingesnė ir atsirado naujų problemų, kurioms spręsti reikia pritaikytų, koordinuotų ir novatoriškų atsakomųjų veiksmų visose valstybėse narėse. Incidentų skaičius, mastas, sudėtingumas, dažnumas ir poveikis didėja bei kelia didelę grėsmę tinklų ir informacinių sistemų veikimui. Todėl incidentai gali trukdyti vykdyti ekonominę veiklą vidaus rinkoje, sukelti finansinių nuostolių, pakirsti naudotojų pasitikėjimą ir padaryti didelę žalą

([1]) OL C 233, 2022 6 16, p. 22.
([2]) OL C 286, 2021 7 16, p. 170.
([3]) 2022 m. lapkričio 10 d. Europos Parlamento pozicija (dar nepaskelbta Oficialiajame leidinyje) ir 2022 m. lapkričio 28 d. Tarybos sprendimas.
([4]) 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (OL L 194, 2016 7 19, p. 1).

Sąjungos ekonomikai ir visuomenei. Todėl kibernetinio saugumo parengtis ir veiksmingumas kaip niekad anksčiau yra labai svarbūs tinkamam vidaus rinkos veikimui. Be to, kibernetinis saugumas yra daugelio ypatingos svarbos sektorių pagrindinė įgalinanti priemonė siekiant sėkmingai vykdyti skaitmeninę transformaciją ir visapusiškai pasinaudoti skaitmeninimo teikiama ekonomine, socialine ir tvarumo nauda;

(4) Direktyvos (ES) 2016/1148 teisinis pagrindas buvo Sutarties dėl Europos Sąjungos veikimo (SESV) 114 straipsnis, kurio tikslas – tobulinant nacionalinių taisyklių suderinimo priemones sukurti vidaus rinką ir užtikrinti jos veikimą. Subjektams, teikiantiems ekonomiškai svarbias paslaugas arba vykdantiems ekonomiškai svarbią veiklą, nustatyti kibernetinio saugumo reikalavimai valstybėse narės gerokai skiriasi atsižvelgiant į reikalavimų rūšį, jų išsamumo lygį ir priežiūros metodą. Dėl tų skirtumų patiriama papildomų išlaidų, o prekes ar paslaugas tarpvalstybiniu mastu tiekiantiems ar tiekiantiems subjektams kyla sunkumų. Vienos valstybės narės nustatyti reikalavimai, kurie skiriasi nuo kitos valstybės narės nustatytų reikalavimų arba net jiems prieštarauja, gali daryti didelį poveikį tokiai tarpvalstybinei veiklai. Be to, tikėtina, kad dėl netinkamos kibernetinio saugumo reikalavimų struktūros arba įgyvendinimo vienoje valstybėje narėje kils pasekmių kitų valstybių narių kibernetinio saugumo lygiui, visų pirma atsižvelgiant į tarpvalstybinių mainų intensyvumą. Atlikus Direktyvos (ES) 2016/1148 peržiūrą, paaiškėjo, kad valstybėse narėse ji įgyvendinama labai įvairiai, be kita ko, kiek tai susiję su jos taikymo sritimi, nes jos ribų nustatymo klausimas iš esmės buvo paliktas valstybių narių diskrecijai. Direktyva (ES) 2016/1148 valstybėms narėms taip pat buvo suteikta labai plati diskrecija dėl joje nustatytų saugumo pareigų ir pranešimų apie incidentus teikimo pareigų įgyvendinimo. Todėl tos pareigos nacionaliniu lygmeniu buvo įgyvendintos labai skirtingai. Panašių skirtumų yra ir Direktyvos (ES) 2016/1148 nuostatų dėl priežiūros ir vykdymo užtikrinimo įgyvendinimo srityje;

(5) visi šie skirtumai lemia vidaus rinkos susiskaidymą ir gali daryti neigiamą poveikį vidaus rinkos veikimui, visų pirma tai pasakytina apie poveikį tarpvalstybiniam paslaugų teikimui ir kibernetinio atsparumo lygiui, kurį lemia taikomos įvairios priemonės. Galiausiai dėl tų skirtumų kai kurios valstybės narės galėtų tapti labiau pažeidžiamos kibernetinių grėsmių atžvilgiu, o tai gali daryti šalutinį poveikį visoje Sąjungoje. Šia direktyva siekiama pašalinti tokius didelius skirtumus tarp valstybių narių, visų pirma nustatant būtiniausias taisykles, susijusias su koordinuotos reguliavimo sistemos veikimu, sukuriant kiekvienos valstybės narės atsakingų institucijų veiksmingo bendradarbiavimo mechanizmus, atnaujinant sektorių ir veiklos, kuriems taikomos kibernetinio saugumo pareigos, sąrašą ir numatant veiksmingas taisomąsias ir vykdymo užtikrinimo priemones, kurios yra labai svarbios veiksmingam tų pareigų vykdymui užtikrinti. Todėl Direktyva (ES) 2016/1148 turėtų būti panaikinta ir pakeista šia direktyva;

(6) panaikinus Direktyvą (ES) 2016/1148, taikymo sritis sektoriams turėtų būti praplėsta, kad apimtų platesnį ekonomikos veiklų spektrą, kad apimtų visus sektorius ir paslaugas, kurie yra nepaprastai svarbūs pagrindinei visuomeninei ir ekonominei veiklai vidaus rinkoje. Visų pirma šia direktyva siekiama pašalinti trūkumus, susijusius su esminių paslaugų operatorių ir skaitmeninių paslaugų teikėjų diferencijacija, kuri yra pasenusi, nes neatspindi sektorių arba paslaugų svarbos visuomeninei ir ekonominei veiklai vidaus rinkoje;

(7) pagal Direktyvą (ES) 2016/1148 valstybės narės buvo atsakingos už subjektų, atitinkančių esminių paslaugų operatoriams taikomus kriterijus, identifikavimą. Siekiant tuo atžvilgiu pašalinti didelius valstybių narių skirtumus ir visiems atitinkamiems subjektams užtikrinti teisinį tikrumą kibernetinio saugumo rizikos valdymo priemonių ir pareigų pranešti atžvilgiu, turėtų būti nustatytas vienas kriterijus, kuriuo remiantis nustatomi subjektai, kurie patenka į šios direktyvos taikymo sritį. Tas kriterijus turėtų būti grindžiamas dydžio ribos taisykle, pagal kurią į šios direktyvos taikymo sritį patenka visi subjektai, kurie laikomi vidutinėmis įmonėmis pagal Komisijos rekomendacijos 2003/361/EB ([5]) priedo 2 straipsnį arba kurie viršija to straipsnio 1 dalyje nustatytas viršutines ribas, ir veikiantys sektoriuose bei teikiantys atitinkamų rūšių paslaugas ar vykdantys veiklą, kuriems taikoma ši direktyva. Valstybės

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

narės taip pat turėtų numatyti, kad į šios direktyvos taikymo sritį patenka tam tikros mažosios įmonės ir labai mažos įmonės, kaip tai apibrėžta to priedo 2 straipsnio 2 ir 3 dalyse, kurios atitinka specifinius kriterijus, pagal kuriuos parodomas jų esminis vaidmuo visuomenei, ekonomikai arba konkretiems sektoriams ar paslaugų rūšims;

(8) ši direktyva neturėtų būti taikoma viešojo administravimo subjektams, kurių veikla daugiausia vykdoma nacionalinio saugumo, visuomenės saugumo, gynybos ar teisėsaugos srityse, įskaitant nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas. Tačiau ši direktyva turėtų būti taikoma viešojo administravimo subjektams, kurių veikla su tomis sritimis susijusi tik nežymiai. Šios direktyvos tikslais reguliavimo kompetenciją turintys subjektai nelaikomi subjektais, vykdančiais veiklą teisėsaugos srityje, todėl ši direktyva nėra jiems netaikoma tuo pagrindu. Ši direktyva netaikoma viešojo administravimo subjektams, įsteigtiems kartu su trečiąja valstybe pagal tarptautinį susitarimą. Ši direktyva netaikoma valstybių narių diplomatinėms ir konsulinėms atstovybėms trečiosiose valstybėse arba jų tinklų ir informacinėms sistemoms, jeigu tokios sistemos yra atstovybės patalpose arba naudojamos naudotojų labui trečiojoje valstybėje;

(9) valstybės narės turėtų galėti imtis priemonių, būtinų esminiams nacionalinio saugumo interesams užtikrinti, viešajai tvarkai palaikyti bei visuomenės saugumui užtikrinti, ir priemonių, kurios leistų sudaryti sąlygas vykdyti nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas. Tuo tikslu valstybės narės turėtų turėti galimybę atleisti konkrečius subjektus, vykdančius veiklą nacionalinio saugumo, visuomenės saugumo, gynybos ar teisėsaugos srityse, įskaitant nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas, nuo tam tikrų šioje direktyvoje nustatytų pareigų tos veiklos atžvilgiu. Kai subjektas teikia paslaugas išimtinai viešojo administravimo subjektui, kuriam ši direktyva netaikoma, valstybės narės turėtų turėti galimybę atleisti tą subjektą nuo tam tikrų šioje direktyvoje nustatytų pareigų tų paslaugų atžvilgiu. Be to, iš jokios valstybės narės neturi būti reikalaujama teikti informacijos, kurios atskleidimas, jos nuomone, prieštarautų esminiams jos nacionalinio saugumo, viešojo saugumo ar gynybos interesams. Tame kontekste turėtų būti atsižvelgiama į Sąjungos arba nacionalines taisykles dėl įslaptintos informacijos apsaugos, susitarimus dėl informacijos neatskleidimo ir neoficialius susitarimus dėl informacijos neatskleidimo, pavyzdžiui, Srauto kontrolės protokolą. Srauto kontrolės protokolas turi būti suprantamas kaip priemonė informacijai apie bet kokius apribojimus, taikomus tolesnei informacijos sklaidai, teikti. Jį naudoja beveik visos reagavimo į kompiuterinius saugumo incidentus tarnybos (toliau – CSIRT) ir kai kurie informacijos analizės ir dalijimosi informacija centrai;

(10) nors ši direktyva taikoma subjektams, vykdantiems elektros energijos gamybos atominėse elektrinėse veiklą, dalis šios veiklos gali būti susijusi su nacionaliniu saugumu. Tokiu atveju valstybė narė, laikydamasi Sutarčių, turėtų turėti galimybę vykdyti savo pareigą užtikrinti savo nacionalinį saugumą, kiek tai susiję su ta veikla, įskaitant veiklą branduolinio sektoriaus vertės grandinėje;

(11) kai kurie subjektai vykdo veiklą nacionalinio saugumo, visuomenės saugumo, gynybos ar teisėsaugos srityse, įskaitant nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas, taip pat teikia patikimumo užtikrinimo paslaugas. Patikimumo užtikrinimo paslaugų teikėjai, kuriems taikomas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 ([6]), turėtų būti įtraukti į šios direktyvos taikymo sritį, kad būtų užtikrintas toks pat saugumo reikalavimų ir priežiūros lygis, koks anksčiau tame reglamente buvo nustatytas patikimumo užtikrinimo paslaugų teikėjų atžvilgiu. Atsižvelgiant į tai, kad Reglamentas (ES) Nr. 910/2014 netaikomas tam tikroms konkrečioms paslaugoms, ši direktyva neturėtų būti taikoma patikimumo užtikrinimo paslaugų, kuriomis naudojamasi tik uždarose sistemose, sukurtose pagal nacionalinę teisę arba apibrėžtos dalyvių grupės susitarimus, teikimui;

([6]) 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).

(12) pašto paslaugų teikėjams, kaip apibrėžta Europos Parlamento ir Tarybos direktyvoje 97/67/EB ([7]), įskaitant kurjerių paslaugų teikėjus, ši direktyva turėtų būti taikoma, jeigu jie teikia paslaugas bent viename pašto paslaugų teikimo grandinės etape, ypač pašto siuntų surinkimo, rūšiavimo, vežimo arba paskirstymo etape, įskaitant siuntų paėmimo paslaugas, atsižvelgiant į jų priklausomumo nuo tinklų ir informacinių sistemų laipsnį. Teikiamos vežimo paslaugos, kai jos nėra susijusios su vienu iš tų etapų, neturėtų patekti į pašto paslaugų apibrėžtį;

(13) dėl intensyvėjančių įkibernetinių grėsmių ir didėjančio sudėtingumo valstybės narės turėtų stengtis užtikrinti, kad subjektai, kuriems netaikoma ši direktyva, pasiektų aukštą kibernetinio saugumo lygį, ir remti lygiaverčių kibernetinio saugumo rizikos valdymo priemonių, atspindinčių jautrų tų subjektų pobūdį, įgyvendinimą;

(14) pagal šią direktyvą vykdomam asmens duomenų tvarkymui taikoma Sąjungos duomenų apsaugos teisė ir Sąjungos privatumo teisė. Visų pirma, šia direktyva nedaromas poveikis Europos Parlamento ir Tarybos reglamentui (ES) 2016/679 ([8]) ir Europos Parlamento ir Tarybos direktyvai 2002/58/EB ([9]). Todėl šia direktyva neturėtų būti daromas poveikis, *inter alia*, institucijų, kurios yra kompetentingos kontroliuoti, kaip laikomasi taikytinos Sąjungos duomenų apsaugos teisės ir Sąjungos privatumo teisės, užduotims ir įgaliojimams;

(15) atitikties kibernetinio saugumo rizikos valdymo priemonėms ir pranešimų teikimo tikslu subjektai, kurie patenka į šios direktyvos taikymo sritį, turėtų būti skirstomi į dvi kategorijas: esminiai subjektai ir svarbūs subjektai, atspindint jų svarbos mastą jų sektoriaus arba jų teikiamų paslaugų rūšies, taip pat jų dydžio požiūriais. Tuo atžvilgiu, kai taikytina, turėtų būti tinkamai atsižvelgiama į visus atitinkamus kompetentingų institucijų atliktus sektorių rizikos vertinimus ar pateiktas gaires. Abiejų kategorijų subjektams taikomi priežiūros ir vykdymo užtikrinimo režimai turėtų būti diferencijuojami siekiant užtikrinti tinkamą, viena vertus, rizika grindžiamų reikalavimų ir pareigų ir, kita vertus, administracinės naštos, atsirandančios dėl atitikties priežiūros, pusiausvyrą;

(16) siekiant kad subjektai, turintys įmonių partnerių arba kurie yra susijusios įmonės, nebūtų laikomi esminiais arba svarbiais subjektais, kai tai būtų neproporcinga, valstybės narės, taikydamos Rekomendacijos 2003/361/EB priedo 6 straipsnio 2 dalį, gali atsižvelgti į subjekto nepriklausomumo nuo savo įmonės partnerės ar susijusių įmonių lygį. Visų pirma valstybės narės gali atsižvelgti į tai, kad subjektas yra nepriklausomas nuo savo įmonės partnerės ar susijusių įmonių kalbant apie tinklų ir informacines sistemas, kuriomis tas subjektas naudojasi teikdamas savo paslaugas, ir kalbant apie subjekto teikiamas paslaugas. Tuo remdamosi, kai tinkama, valstybės narės gali laikyti, kad toks subjektas negali būti laikomas vidutine įmone pagal Komisijos rekomendacijos 2003/361/EB priedo 2 straipsnį arba kad jis neviršija to straipsnio 1 dalyje vidutinei įmonei nustatytų viršutinių ribų, jeigu, atsižvelgus į to subjekto nepriklausomumo lygį, tas subjektas nebūtų laikomas vidutine įmone arba jis neviršytų tų viršutinių ribų tuo atveju, jei būtų atsižvelgiama tik į jo paties duomenis. Tai nedaro poveikio šioje direktyvoje nustatytoms įmonių partnerių ir susijusių įmonių, kurioms taikoma ši direktyva, pareigoms;

(17) valstybės narės turėtų galėti nuspręsti, kad subjektai, kurie prieš šios direktyvos įsigaliojimą buvo identifikuoti kaip esminių paslaugų operatoriai pagal Direktyvą (ES) 2016/1148, būtų laikomi esminiais subjektais;

([7]) 1997 m. gruodžio 15 d. Europos Parlamento ir Tarybos direktyva 97/67/EB dėl Bendrijos pašto paslaugų vidaus rinkos plėtros bendrųjų taisyklių ir paslaugų kokybės gerinimo (OL L 15, 1998 1 21, p. 14).

([8]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1).

([9]) 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 37).

(18) siekdamos užtikrinti aiškią subjektų, kuriems taikoma ši direktyva, apžvalgą, valstybės narės turėtų sudaryti esminių ir svarbių subjektų bei domenų vardų registravimo paslaugas teikiančių subjektų sąrašą. Tuo tikslu valstybės narės turėtų reikalauti, kad subjektai kompetentingoms institucijoms pateiktų bent šią informaciją: subjekto pavadinimą, adresą ir naujausius kontaktinius duomenis, įskaitant el. pašto adresus, IP adresus ir telefono numerius, ir, kai taikytina, atitinkamą sektorių ir subsektorių, nurodytus prieduose, taip pat, kai taikytina, valstybių narių, kuriose jie teikia paslaugas, kurioms taikoma ši direktyva, sąrašą. Tuo tikslu Komisija, padedant Europos Sąjungos kibernetinio saugumo agentūrai (toliau – ENISA), nepagrįstai nedelsdama turėtų pateikti gaires ir šablonus dėl pareigos teikti informaciją. Siekiant sudaryti palankesnes sąlygas sukurti ir atnaujinti esminių ir svarbių subjektų bei domenų vardų registravimo paslaugas teikiančių subjektų sąrašą, valstybės narės turėtų turėti galimybę nustatyti nacionalinius mechanizmus, kuriuos taikant subjektai galėtų užsiregistruoti patys. Tais atvejais, kai nacionaliniu lygmeniu registrai jau yra sukurti, valstybės narės gali nuspręsti dėl tinkamų mechanizmų, kuriais sudaroma galimybė identifikuoti subjektus, kuriems taikoma ši direktyva;

(19) valstybės narės turėtų būti atsakingos už tai, kad Komisijai būtų pateiktas bent kiekvieno prieduose nurodyto sektoriaus ir subsektoriaus esminių ir svarbių subjektų skaičius, taip pat atitinkama informacija apie identifikuotų subjektų skaičių ir šioje direktyvoje numatyta nuostata, pagal kurią jie buvo identifikuoti, ir jų teikiamos paslaugos rūšį. Valstybės narės raginamos keistis su Komisija informacija apie esminius ir svarbius subjektus, o didelio masto kibernetinio saugumo incidento atveju – atitinkama informacija, pavyzdžiui, apie atitinkamo subjekto pavadinimą;

(20) Komisija, bendradarbiaudama su Bendradarbiavimo grupe ir pasikonsultavusi su atitinkamais suinteresuotaisiais subjektais, turėtų pateikti labai mažoms ir mažosioms įmonėms taikomų kriterijų įgyvendinimo gaires įvertinimo, ar jos patenka į šios direktyvos taikymo sritį, tikslais. Komisija taip pat turėtų užtikrinti, kad atitinkamos gairės būtų pateiktos labai mažoms ir mažosioms įmonėms, kurioms taikoma ši direktyva. Komisija, padedant valstybėms narėms, turėtų pateikti labai mažoms ir mažosioms įmonėms informacijos tuo klausimu;

(21) Komisija galėtų pateikti gaires, skirtas padėti valstybėms narėms įgyvendinti šios direktyvos nuostatas dėl taikymo srities ir įvertinti priemonių, kurių turi būti imamasi pagal šią direktyvą, proporcingumą, visų pirma atsižvelgiant į subjektus, kurių verslo modeliai arba veiklos aplinka yra sudėtingi, kai subjektas vienu metu gali atitikti ir esminiams, ir svarbiems subjektams nustatytus kriterijus arba gali tuo pačiu metu vykdyti veiklą, kurios dalis patenka į šios direktyvos taikymo sritį, o dalis nepatenka;

(22) šioje direktyvoje nustatomi kibernetinio saugumo rizikos valdymo priemonių ir pareigų pranešti, taikomų į jos taikymo sritį patenkančiuose sektoriuose, pagrindai. Siekiant išvengti Sąjungos teisės aktų nuostatų dėl kibernetinio saugumo susiskaidymo, kai manoma, kad, siekiant užtikrinti aukšto lygio kibernetinį saugumą visoje Sąjungoje, reikalingi tolesni konkretiems sektoriams taikomi Sąjungos teisės aktai, susiję su kibernetinio saugumo rizikos valdymo priemonėmis ir pareigomis pranešti, Komisija turėtų įvertinti, ar tokios tolesnės nuostatos galėtų būti nustatytos pagal šią direktyvą priimame įgyvendinimo akte. Jei toks įgyvendinimo aktas būtų netinkamas tam tikslui, konkretiems sektoriams taikomi Sąjungos teisės aktai galėtų padėti užtikrinti aukšto lygio kibernetinį saugumą visoje Sąjungoje, visapusiškai atsižvelgiant į atitinkamų sektorių specifiką ir sudėtingumą. Tuo tikslu šia direktyva nedraudžiama priimti tolesnių konkretiems sektoriams taikomų Sąjungos teisės aktų, kuriais reglamentuojamos kibernetinio saugumo rizikos valdymo priemonės ir pareigos pranešti ir kuriais tinkamai atsižvelgiama į poreikį sukurti visapusišką bei nuoseklią kibernetinio saugumo sistemą. Šia direktyva nedaromas poveikis dabartiniams įgyvendinimo įgaliojimams, kurie Komisijai suteikti įvairiuose sektoriuose, įskaitant transporto ir energetikos sektorius;

(23) jei konkrečiam sektoriui taikomame Sąjungos teisės akte yra nuostatos, pagal kurias reikalaujama, kad esminiai arba svarbūs subjektai priimtų kibernetinio saugumo rizikos valdymo priemones arba praneštų apie didelius incidentus, ir jei tų reikalavimų poveikis yra bent lygiavertis šioje direktyvoje nustatytų pareigų poveikiui, tos nuostatos,

įskaitant nuostatas dėl priežiūros ir vykdymo užtikrinimo, turėtų būti taikomos tokiems subjektams. Jei konkrečiam sektoriui taikomas Sąjungos teisės aktas taikomas ne visiems konkretaus sektoriaus, kuriam taikoma ši direktyva, subjektams, atitinkamos šios direktyvos nuostatos turėtų būti toliau taikomos subjektams, kuriems netaikomas tas aktas;

(24) jei pagal konkrečiam sektoriui taikomo Sąjungos teisės akto nuostatas reikalaujama, kad esminiai arba svarbūs subjektai laikytųsi pareigų pranešti, kurių poveikis yra bent lygiavertis šioje direktyvoje nustatytų pareigų pranešti poveikiui, turėtų būti užtikrintas pranešimų apie incidentus tvarkymo nuoseklumas ir veiksmingumas. Tuo tikslu konkrečiam sektoriui taikomo Sąjungos teisės akto nuostatomis dėl pranešimo apie incidentus turėtų būti suteikta galimybė CSIRT, kompetentingoms institucijoms arba bendriesiems kibernetinio saugumo kontaktiniams punktams (toliau – bendrieji kontaktiniai punktai) pagal šią direktyvą nedelsiant susipažinti su pranešimais apie incidentus, pateiktais pagal konkrečiam sektoriui taikomą Sąjungos teisės aktą. Visų pirma tokia neatidėliotina prieiga gali būti užtikrinta, jei pranešimai apie incidentus nepagrįstai nedelsiant persiunčiami CSIRT, kompetentingai institucijai arba bendrajam kontaktiniam punktui pagal šią direktyvą. Prireikus valstybės narės turėtų įdiegti automatinį tiesioginio pranešimo mechanizmą, kuriuo būtų užtikrinamas sistemingas ir neatidėliotinas keitimasis informacija su CSIRT, kompetentingomis institucijomis arba bendruoju kontaktiniu punktu dėl tokių pranešimų apie incidentus tvarkymo. Siekdamos supaprastinti pranešimų teikimą ir įgyvendinti automatinį tiesioginio pranešimo mechanizmą, valstybės narės, vadovaudamosi konkrečiam sektoriui taikomu Sąjungos teisės aktu, galėtų naudotis viena bendra prieiga;

(25) konkretiems sektoriams taikomuose Sąjungos teisės aktuose, pagal kuriuos numatytos kibernetinio saugumo rizikos valdymo priemonės arba pareigos pranešti, kurių poveikis yra bent lygiavertis šioje direktyvoje numatytų priemonių ar pareigų poveikiui, galėtų būti nustatyta, kad kompetentingos institucijos pagal tokius aktus savo priežiūros ir vykdymo užtikrinimo įgaliojimais, susijusiais su tokiomis priemonėmis arba pareigomis, naudojasi padedant kompetentingoms institucijoms pagal šią direktyvą. Atitinkamos kompetentingos institucijos tuo tikslu galėtų sudaryti bendradarbiavimo susitarimus. Tokiuose bendradarbiavimo susitarimuose, *inter alia*, galėtų būti nustatytos priežiūros veiklos koordinavimo procedūros, įskaitant tyrimų ir patikrinimų vietoje procedūras laikantis nacionalinės teisės, ir kompetentingų institucijų keitimosi atitinkama informacija apie priežiūrą ir vykdymo užtikrinimą mechanizmas, be kita ko, prieiga prie su kibernetine sritimi susijusios informacijos, kurios prašo tos kompetentingos institucijos pagal šią direktyvą;

(26) jei pagal konkretiems sektoriams taikomus Sąjungos teisės aktus reikalaujama, kad subjektai praneštų apie dideles kibernetines grėsmes arba skatinama, kad jie tai darytų, valstybės narės taip pat turėtų skatinti dalytis informacija apie dideles kibernetines grėsmes su CSIRT, kompetentingomis institucijomis arba bendraisiais kontaktiniais punktais pagal šią direktyvą, siekiant užtikrinti didesnį tų įstaigų informuotumą apie kibernetinių grėsmių padėtį ir sudaryti joms galimybę veiksmingai bei laiku reaguoti, jei didelės kibernetinės grėsmės pasireikštų;

(27) būsimuose konkretiems sektoriams taikomuose Sąjungos teisės aktuose turėtų būti tinkamai atsižvelgta į šioje direktyvoje nustatytas terminų apibrėžtis ir priežiūros bei vykdymo užtikrinimo sistemą;

(28) Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 ([10]) turėtų būti vertinamas kaip konkrečiam sektoriui taikomas Sąjungos teisės aktas šios direktyvos atžvilgiu, kiek tai susiję su finansų sektoriaus subjektais. Reglamento (ES) 2022/2554 nuostatos, susijusios su informacinių ir ryšių technologijų (IRT) rizikos valdymu, su IRT susijusių incidentų valdymu, ypač pranešimų apie didelius su IRT susijusius incidentus teikimu, taip pat su skaitmeninės veiklos atsparumo testavimu, dalijimosi informacija susitarimais ir trečiosios šalies IRT rizika, turėtų būti taikomos vietoj šioje direktyvoje įtvirtintų nuostatų. Todėl valstybės narės šios direktyvos nuostatų dėl kibernetinio saugumo rizikos valdymo ir pareigų pranešti bei priežiūros ir vykdymo užtikrinimo neturėtų taikyti finansų sektoriaus subjektams, kuriems taikomas Reglamentas (ES) 2022/2554. Kartu pagal šią direktyvą svarbu išlaikyti tvirtus ryšius su finansų sektoriumi ir užtikrinti, kad su juo būtų keičiamasi informacija. Tuo tikslu Reglamentu (ES) 2022/2554 Europos priežiūros institucijoms (EPI) ir kompetentingoms institucijoms pagal tą reglamentą leidžiama dalyvauti Bendradarbiavimo grupės veikloje ir keistis informacija bei bendradarbiauti su bendraisiais kontaktiniais punktais, taip pat CSIRT ir kompetentingomis institucijomis pagal šią direktyvą. Kompetentingos institucijos pagal Reglamentą (ES) 2022/2554 CSIRT, kompetentingoms institucijoms arba bendriesiems kontaktiniams punktams pagal šią direktyvą taip pat turėtų perduoti išsamius duomenis apie didelius su IRT susijusius incidentus ir, kai

([10]) 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011 (žr. šio Oficialiojo leidinio p.1).

tinkama, dideles kibernetines grėsmes. Tai galima pasiekti suteikiant neatidėliotiną prieigą prie pranešimų apie incidentus ir juos perduodant, tiesiogiai arba per vieną bendrą prieigą. Be to, valstybės narės į savo kibernetinio saugumo strategijas turėtų toliau įtraukti finansų sektorių, o CSIRT savo veikloje gali aptarti finansų sektoriaus klausimus;

(29) siekiant išvengti kibernetinio saugumo pareigų, nustatytų aviacijos sektoriaus subjektams, spragų ar šių pareigų dubliavimosi, nacionalinės institucijos pagal Europos Parlamento ir Tarybos reglamentus (EB) Nr. 300/2008 ([11]) ir (ES) 2018/1139 ([12]) ir kompetentingos institucijos pagal šią direktyvą turėtų bendradarbiauti įgyvendindamos kibernetinio saugumo rizikos valdymo priemones ir vykdydamos atitikties toms priemonėms priežiūrą nacionaliniu lygmeniu. Kompetentingos institucijos pagal šią direktyvą galėtų laikyti, kad subjekto atitiktis saugumo reikalavimams, nustatytiems reglamentuose (EB) Nr. 300/2008 ir (ES) 2018/1139 bei atitinkamuose pagal tuos reglamentus priimtuose deleguotuosiuose ir įgyvendinimo aktuose, yra atitiktis atitinkamiems šioje direktyvoje nustatytiems reikalavimams;

(30) atsižvelgiant į kibernetinio saugumo ir subjektų fizinio saugumo tarpusavio ryšius, reikėtų užtikrinti nuoseklų požiūrį tarp Europos Parlamento ir Tarybos direktyvos (ES) 2022/2557 ([13]) ir šios direktyvos. Kad būtų pasiektas šis tikslas, subjektai, identifikuoti kaip ypatingos svarbos subjektai pagal Direktyvą (ES) 2022/2557, turėtų būti laikomi esminiais subjektais pagal šią direktyvą. Be to, kiekviena valstybė narė turėtų užtikrinti, kad jos nacionalinėje kibernetinio saugumo strategijoje būtų numatyta politikos sistema, pagal kurią toje valstybėje narėje būtų numatytas tvirtesnis jos kompetentingų institucijų pagal šią direktyvą ir kompetentingų institucijų pagal Direktyvą (ES) 2022/2557 veiklos koordinavimas keičiantis informacija apie riziką, kibernetines grėsmes, ir incidentus, taip pat nekibernetinę riziką, grėsmes bei incidentus, taip pat vykdant priežiūros užduotis. Kompetentingos institucijos pagal šią direktyvą ir pagal Direktyvą (ES) 2022/2557 turėtų bendradarbiauti ir keistis informacija nepagrįstai nedelsdamos, visų pirma kiek tai susiję su ypatingos svarbos subjektų identifikavimu, rizika, kibernetinėmis grėsmėmis, ir incidentais, taip pat su nekibernetine rizika, grėsmėmis ir incidentais, darančiais poveikį ypatingos svarbos subjektams, įskaitant kibernetinio saugumo ir fizines priemones, kurių ėmėsi ypatingos svarbos subjektai, taip pat tokių subjektų atžvilgiu vykdomos priežiūros veiklos rezultatais.

Be to, siekiant supaprastinti kompetentingų institucijų pagal šią direktyvą ir pagal Direktyvą (ES) 2022/2557 vykdomą tarpusavio priežiūros veiklą ir kuo labiau sumažinti atitinkamiems subjektams tenkančią administracinę naštą, tos kompetentingos institucijos turėtų stengtis suderinti pranešimo apie incidentus šablonus ir priežiūros procesus. Prireikus kompetentingos institucijos pagal Direktyvą (ES) 2022/2557 turėtų galėti prašyti kompetentingų institucijų pagal šią direktyvą naudotis savo priežiūros ir vykdymo užtikrinimo įgaliojimais subjekto, kuris identifikuotas kaip ypatingos svarbos subjektas pagal Direktyvą (ES) 2022/2557, atžvilgiu. Tuo tikslu kompetentingos institucijos pagal šią direktyvą ir pagal Direktyvą (ES) 2022/2557 turėtų bendradarbiauti ir keistis informacija, kai įmanoma – tikruoju laiku;

(31) skaitmeninės infrastruktūros sektoriaus subjektai iš esmės priklauso nuo tinklų ir informacinių sistemų, todėl pagal šią direktyvą tiems subjektams nustatytomis pareigomis turėtų būti visapusiškai atsižvelgiama į tokių sistemų fizinį saugumą, kaip jų kibernetinio saugumo rizikos valdymo priemonių ir pranešimų teikimo pareigų dalį. Kadangi tiems klausimams taikoma ši direktyva, Direktyvos (ES) 2022/2557 III, IV ir VI skyriuose nustatytos pareigos tokiems subjektams netaikomos;

([11]) 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).

([12]) 2018 m. liepos 4 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1139 dėl bendrųjų civilinės aviacijos taisyklių, ir kuriuo įsteigiama Europos Sąjungos aviacijos saugos agentūra, iš dalies keičiami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 2111/2005, (EB) Nr. 1008/2008, (ES) Nr. 996/2010, (ES) Nr. 376/2014 ir direktyvos 2014/30/ES ir 2014/53/ES bei panaikinami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 552/2004 ir (EB) Nr. 216/2008 bei Tarybos reglamentas (EEB) Nr. 3922/91 (OL L 212, 2018 8 22, p. 1).

([13]) 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2557 dėl ypatingos svarbos subjektų atsparumo, kuria panaikinama Tarybos direktyva 2008/114/EB (žr. šio Oficialiojo leidinio p.164).

(32) patikimos, atsparios ir saugios domenų vardų sistemos (DNS) palaikymas ir išsaugojimas yra pagrindiniai veiksniai užtikrinant interneto vientisumą ir tai yra labai svarbu jos nuolatiniam ir stabiliam veikimui, nuo kurio priklauso skaitmeninė ekonomika ir visuomenė. Todėl ši direktyva turėtų būti taikoma aukščiausio lygio domenų vardų registrams ir DNS paslaugų teikėjams, kurie suprantami kaip subjektai, teikiantys viešai prieinamas rekursinio domenų vardų keitimo paslaugas galutinių interneto naudotojų reikmėms ar patikimo domenų vardų keitimo paslaugas trečiųjų šalių reikmėms. Ši direktyva neturėtų būti taikoma šakninio pavadinimo serveriams;

(33) debesijos kompiuterijos paslaugos turėtų apimti skaitmenines paslaugas, kurios pagal poreikį suteikia administravimo paslaugas ir plataus masto nuotolinę prieigą prie kintamo masto pritaikomos bendrų kompiuterijos išteklių bazės, įskaitant atvejus, kai tokie ištekliai yra paskirstyti per kelias vietas. Kompiuterijos ištekliai apima tokius išteklius, kaip tinklai, serveriai ar kita infrastruktūra, operacinės sistemos, programinė įranga, kaupikliai, taikomosios programos ir paslaugos. Debesijos kompiuterijos paslaugų modeliai, *inter alia*, apima paslauginę infrastruktūrą (IaaS), paslauginę platformą (PaaS), paslauginę programinę įrangą (SaaS) ir paslauginį tinklą (NaaS). Debesijos kompiuterijos diegimo modeliai turėtų apimti privačią, bendrą, viešą ir mišrią debesiją. Debesijos kompiuterijos paslaugos ir diegimo modeliai turi tokią pačią reikšmę kaip ir pagal ISO/IEC 17788:2014 standartą apibrėžti paslaugos sąlygų ir diegimo modeliai. Debesijos kompiuterijos naudotojo gebėjimas vienašališkai pasirūpinti kompiuterijos pajėgumais, pavyzdžiui, serverio laiku arba tinklo saugykla, be jokio žmogaus įsikišimo, atliekamo debesijos kompiuterijos paslaugų teikėjo, galėtų būti apibūdinamas kaip administravimas pagal poreikį.

Terminas „plataus masto nuotolinė prieiga“ naudojamas apibūdinant debesijos pajėgumus, kurie užtikrinami tinkle ir kuriais galima pasinaudoti per mechanizmus, kuriais skatinamas įvairių mažafunkcių arba daugiafunkcių kompiuterių platformų, įskaitant mobiliuosius telefonus, planšetinius kompiuterius, knyginius kompiuterius ir profesionaliuosius kompiuterius, naudojimas. Terminas „kintamo masto“ reiškia, kad atsižvelgdamas į paklausos svyravimus, debesijos paslaugų teikėjas lanksčiai paskirsto kompiuterijos išteklius nepriklausomai nuo geografinės išteklių vietos. Terminas „pritaikoma bazė“ reiškia, kad siekiant sparčiai padidinti ir sumažinti turimus kompiuterijos išteklius pagal darbo krūvį, tais ištekliais aprūpinama ir jie yra tiekiami atsižvelgiant į paklausą. Terminas „bendri“ reiškia, kad kompiuterijos ištekliai yra tiekiami keliems naudotojams, kurie dalijasi bendra prieiga prie paslaugos, tačiau tie ištekliai tvarkomi atskirai kiekvieno naudotojo atveju, nors paslauga yra teikiama naudojant tą pačią elektroninę įrangą. Terminas „paskirstyti“ reiškia kompiuterijos išteklius, kurie yra skirtinguose tinkliniuose kompiuteriuose ar prietaisuose ir kurie tarpusavyje bendrauja ir koordinuoja perduodami pranešimus;

(34) atsižvelgiant į novatoriškų technologijų ir naujų verslo modelių atsiradimą, tikimasi, kad vidaus rinkoje atsiras naujų debesijos kompiuterijos paslaugų ir diegimo modelių, atsižvelgiant į kintančius vartotojų poreikius. Šiomis aplinkybėmis debesijos kompiuterijos paslaugos gali būti teikiamos labai paskirstyta forma, dar arčiau duomenų generavimo ar rinkimo vietos, taip pereinant nuo tradicinio modelio prie labai paskirstyto modelio (tinklo paribio kompiuterija);

(35) duomenų centro paslaugų teikėjų siūlomos paslaugos ne visada gali būti teikiamos debesijos kompiuterijos paslaugos forma. Taigi, duomenų centrai ne visada gali priklausyti debesijos kompiuterijos infrastruktūrai. Siekiant valdyti visą riziką, kuri kyla tinklų ir informacinių sistemų saugumui, ši direktyva turėtų būti taikoma duomenų centrų paslaugų, kurios nėra debesijos kompiuterijos paslaugos, teikėjams. Taikant šią direktyvą, sąvoka „duomenų centro paslauga“ turėtų apimti paslaugos, kuri apima struktūras arba struktūrų grupes, skirtas informacinių technologijų (IT) ir tinklo įrangos centralizuotam pritaikymui, tarpusavio junglumui ir eksploatavimui, teikiant duomenų saugojimo, tvarkymo ir transportavimo paslaugas kartu su visa energijos paskirstymo ir aplinkos kontrolės įranga ir infrastruktūra, teikimą. Sąvoka „duomenų centro paslauga“ neturėtų būti taikoma vidaus korporatyviniams duomenų centrams, kurie priklauso atitinkamam subjektui ir yra jo eksploatuojami to subjekto reikmėms;

(36) vienas iš svarbiausių vaidmenų kuriant naujus produktus ir procesus tenka tyrimų veiklai. Didžiąją dalį tos veiklos vykdo subjektai, kurie dalijasi savo tyrimų rezultatais, juos platina arba naudoja komerciniais tikslais. Todėl tie subjektai gali būti svarbūs vertės grandinių dalyviai, o jų tinklų ir informacinių sistemų saugumas yra neatsiejama bendro vidaus rinkos kibernetinio saugumo dalis. Tyrimų organizacijos turėtų būti suprantamos kaip apimančios subjektus, kurie pagrindinę dalį savo veiklos skiria taikomųjų mokslinių tyrimų arba eksperimentinės plėtros

vykdymui, kaip tai suprantama 2015 m. Ekonominio bendradarbiavimo ir plėtros organizacijos Fraskačio vadove: mokslinių tyrimų ir eksperimentinės plėtros duomenų rinkimo ir teikimo gairėse (angl. „Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development“), siekdami panaudoti savo rezultatus komerciniais tikslais, pavyzdžiui, produkto ar proceso gamybos ar kūrimo arba paslaugos teikimo ir jų pateikimo rinkai tikslais;

(37) didėjančią tarpusavio priklausomybę lemia vis labiau tarptautinio pobūdžio ir tarpusavyje priklausomas paslaugų teikimo tinklas, kuriame naudojami pagrindiniai visoje Sąjungoje esantys tokių sektorių kaip energetika, transportas, skaitmeninė infrastruktūra, geriamasis vanduo ir nuotekos, sveikata, tam tikri viešojo administravimo aspektai, taip pat kosmosas, infrastruktūros objektai, kiek tai susiję su tam tikrų paslaugų teikimu, kuriam įtakos turi antžeminės infrastruktūros objektai, kurie priklauso valstybėms narėms arba privačioms šalims, yra jų valdomi arba eksploatuojami, todėl tai neapima infrastruktūros objektų, kurie priklauso Sąjungai, kai ji įgyvendina savo kosmoso programą, arba kurie yra valdomi ar eksploatuojami Sąjungos vardu šios programos įgyvendinimo metu. Ta tarpusavio priklausomybė reiškia, kad bet koks sutrikimas, kuris iš pradžių įvyksta tik viename subjekte arba sektoriuje, gali turėti platesnį grandininį poveikį ir sukelti platesnio masto ir ilgalaikes neigiamas pasekmes paslaugų teikimui visoje vidaus rinkoje. COVID-19 pandemijos metu padažnėję kibernetiniai išpuoliai parodė, kad vis labiau tarpusavyje priklausoma visuomenė yra pažeidžiama atsižvelgiant į mažai tikėtiną riziką;

(38) atsižvelgiant į nacionalinių valdymo struktūrų skirtumus ir siekiant išsaugoti jau veikiančias sektorių sistemas ar Sąjungos priežiūros ir reguliavimo įstaigas, valstybės narės turėtų turėti teisę paskirti ar įsteigti vieną ar daugiau kompetentingų institucijų, atsakingų už užduočių kibernetinio saugumo ir priežiūros srityse pagal šią direktyvą vykdymą;

(39) siekiant palengvinti tarpvalstybinį institucijų bendradarbiavimą ir ryšių palaikymą bei sudaryti sąlygas veiksmingai įgyvendinti šią direktyvą, būtina, kad kiekviena valstybė narė paskirtų bendrąjį kontaktinį punktą, atsakingą už klausimų, susijusių su tinklų ir informacinių sistemų saugumu, koordinavimą ir tarpvalstybinį bendradarbiavimą Sąjungos lygmeniu;

(40) bendrieji kontaktiniai punktai turėtų užtikrinti veiksmingą tarpvalstybinį bendradarbiavimą su atitinkamomis kitų valstybių narių institucijomis ir prireikus su Komisija ir ENISA. Todėl bendriesiems kontaktiniams punktams turėtų būti pavesta, CSIRT arba kompetentingai institucijai paprašius, persiųsti pranešimus apie didelius tarpvalstybinio poveikio incidentus kitų paveiktų valstybių narių bendriesiems kontaktiniams punktams. Nacionaliniu lygmeniu bendrieji kontaktiniai punktai turėtų sudaryti sąlygas sklandžiam tarpsektoriniam bendradarbiavimui su kitomis kompetentingomis institucijomis. Bendrieji kontaktiniai punktai taip pat galėtų gauti atitinkamą informaciją apie incidentus, susijusius su finansų sektoriaus subjektais, iš kompetentingų institucijų pagal Reglamentą (ES) 2022/2554, kurią jie turėtų turėti galimybę, kai tinkama, persiųsti CSIRT arba kompetentingoms institucijoms pagal šią direktyvą;

(41) valstybės narės turėtų būti tinkamai pasirengusios – turėti tiek techninių, tiek organizacinių pajėgumų, kad galėtų užkirsti kelią incidentams bei rizikai, juos atskleisti, į juos reaguoti ir sušvelninti jų poveikį. Todėl valstybės narės turėtų pagal šią direktyvą įsteigti ar paskirti vieną ar daugiau CSIRT ir užtikrinti, kad jos turėtų pakankamai išteklių bei techninių pajėgumų. CSIRT turėtų atitikti šioje direktyvoje nustatytus reikalavimus, kad būtų garantuoti veiksmingi bei suderinami incidentų bei rizikos valdymo pajėgumai ir užtikrintas veiksmingas bendradarbiavimas Sąjungos lygmeniu. Valstybės narės turėtų turėti galimybę CSIRT paskirti jau esamas kompiuterinių incidentų tyrimo tarnybas (CERT). Siekiant stiprinti pasitikėjimu grindžiamus santykius tarp subjektų ir CSIRT, tais atvejais, kai CSIRT veikia kompetentingoje institucijoje, valstybės narės turėtų galėti apsvarstyti galimybę funkciniu požiūriu atskirti CSIRT vykdomas operatyvines užduotis, ypač susijusias su dalijimusi informacija ir subjektams teikiama pagalba, ir kompetentingų institucijų priežiūros veiklą;

(42) CSIRT pavesta valdyti incidentus. Tai apima didelių kartais neskelbtinų duomenų kiekių tvarkymą. Valstybės narės turėtų užtikrinti, kad CSIRT turėtų dalijimosi informacija ir jos tvarkymo infrastruktūrą, taip pat gerai aprūpintą personalą, kuris užtikrintų jų operacijų konfidencialumą ir patikimumą. CSIRT taip pat galėtų priimti elgesio kodeksus šiuo klausimu;

(43) kalbant apie asmens duomenis pažymėtina, kad CSIRT turėtų turėti galimybę pagal Reglamentą (ES) 2016/679 subjekto, kuriam taikoma ši direktyva, prašymu imtis iniciatyvos patikrinti tinklų ir informacines sistemas, naudojamas esminio ar svarbaus subjekto paslaugoms teikti. Jei taikoma, valstybės narės turėtų siekti užtikrinti vienodą visų sektorių CSIRT techninių pajėgumų lygį. Valstybės narės turėtų turėti galimybę paprašyti ENISA padėti kurti jų CSIRT;

(44) CSIRT turėtų turėti galimybę esminio ar svarbaus subjekto prašymu stebėti subjekto su internetu susietus išteklius tiek patalpose, tiek už jų ribų, kad nustatytų, suprastų ir valdytų subjekto bendrą organizacinę riziką, susijusią su naujai nustatytomis tiekimo grandinės spragomis ar kritiniais pažeidžiamumais. Subjektas turėtų būti skatinamas pranešti CSIRT, ar jis naudoja privilegijuotojo valdymo sąsają, nes tai galėtų turėti įtakos rizikos mažinimo veiksmų įgyvendinimo spartai;

(45) atsižvelgiant į tarptautinio bendradarbiavimo kibernetinio saugumo srityje svarbą, CSIRT turėtų turėti galimybę dalyvauti ne tik šia direktyva sukurto CSIRT tinklo, bet ir tarptautinio bendradarbiavimo tinklų veikloje. Todėl siekdamos vykdyti savo užduotis, CSIRT ir kompetentingos institucijos turėtų turėti galimybę keistis informacija, įskaitant asmens duomenis, su trečiųjų valstybių nacionalinėmis reagavimo į kompiuterių saugumo incidentus grupėmis arba kompetentingomis institucijomis, jeigu laikomasi Sąjungos duomenų apsaugos teisės aktuose nustatytų asmens duomenų perdavimo trečiosioms valstybėms sąlygų, *inter alia*, Reglamento (ES) 2016/679 49 straipsnyje nustatytų sąlygų;

(46) norint pasiekti šios direktyvos tikslus ir sudaryti galimybę kompetentingoms institucijoms bei CSIRT vykdyti joje nustatytas užduotis, nepaprastai svarbu užtikrinti pakankamus išteklius. Valstybės narės nacionaliniu lygmeniu gali nustatyti finansavimo mechanizmą, pagal kurį būtų dengiamos būtinos išlaidos, susijusios su už kibernetinį saugumą valstybėje narėje atsakingų viešųjų subjektų užduočių vykdymu pagal šią direktyvą. Toks mechanizmas turėtų atitikti Sąjungos teisę, būti proporcingas ir nediskriminacinis, taip pat juo turėtų būti atsižvelgiama į skirtingus požiūrius į saugių paslaugų teikimą;

(47) CSIRT tinklas turėtų toliau padėti stiprinti valstybių narių tarpusavio pasitikėjimą bei patikimumą ir skatinti spartų ir efektyvų operatyvinį bendradarbiavimą. Siekdamas intensyvinti operatyvinį bendradarbiavimą Sąjungos lygmeniu, CSIRT tinklas turėtų apsvarstyti galimybę pakviesti savo darbe dalyvauti kibernetinio saugumo politikos srityje veikiančius Sąjungos organus ir agentūras, pavyzdžiui, Europolą;

(48) siekiant pasiekti ir išlaikyti aukštą kibernetinio saugumo lygį, nacionalines kibernetinio saugumo strategijas, kurių reikalaujama pagal šią direktyvą, turėtų sudaryti nuoseklios sistemos, kuriose būtų numatyti strateginiai tikslai bei prioritetai kibernetinio saugumo srityje ir jų įgyvendinimo valdymas. Tas strategijas gali sudaryti viena ar daugiau teisėkūros arba ne teisėkūros priemonių;

(49) kibernetinės higienos politikoje numatomi tinklų ir informacinių sistemų infrastruktūros, aparatinės įrangos, programinės įrangos ir internetinių programų saugumo, taip pat subjektų naudojamų verslo ir galutinių naudotojų duomenų apsaugos pagrindai. Kibernetinės higienos politika, apimanti bendrą praktikos pavyzdžių, be kita ko, susijusių su programinės ir aparatinės įrangos atnaujinimu, slaptažodžių keitimu, naujai įdiegtų programų valdymu, administratoriaus lygmens prieigos paskyrų ribojimu ir duomenų atsarginiu kopijavimu, rinkinį, sudaro sąlygas iniciatyviai pasirengimo ir bendros saugos bei saugumo incidentų ar kibernetinių grėsmių atveju sistemai. ENISA turėtų stebėti ir analizuoti valstybių narių kibernetinės higienos politiką;

(50) informuotumas apie kibernetinį saugumą ir kibernetinė higiena yra nepaprastai svarbūs siekiant padidinti kibernetinio saugumo lygį Sąjungoje, visų pirma atsižvelgiant į didėjantį prijungtųjų įrenginių, kurie vis dažniau naudojami kibernetinių išpuolių metu, skaičių. Reikėtų dėti pastangas siekiant didinti bendrą informuotumą apie riziką, susijusią su tokiais įrenginiais, o vertinimai Sąjungos lygmeniu galėtų padėti užtikrinti bendrą supratimą apie tokią riziką vidaus rinkoje;

(51) valstybės narės turėtų skatinti naudoti visas novatoriškas technologijas, įskaitant dirbtinį intelektą, kurias naudojant galėtų būti geriau atskleidžiami kibernetiniai išpuoliai ir geriau jų išvengiama, sudarant sąlygas veiksmingiau nukreipti išteklius kovai su kibernetiniais išpuoliais. Todėl valstybės narės savo nacionalinėje kibernetinio saugumo strategijoje turėtų skatinti tyrimų ir plėtros veiklą, kad būtų sudarytos palankesnės sąlygos naudoti tokias technologijas, visų pirma susijusias su automatizuotomis arba pusiau automatizuotomis kibernetinio saugumo priemonėmis, ir prireikus dalytis duomenimis, kurių reikia tokių technologijų naudotojams mokyti ir joms tobulinti. Bet kokių novatoriškų technologijų, įskaitant dirbtinį intelektą, naudojimas turėtų atitikti Sąjungos duomenų apsaugos teisės aktus, įskaitant tokius duomenų apsaugos principus, kaip duomenų tikslumo, duomenų kiekio mažinimo, sąžiningumo ir skaidrumo, taip pat duomenų saugumo, pavyzdžiui, pažangiausio šifravimo. Turėtų būti visapusiškai naudojamasi Reglamente (ES) 2016/679 nustatytais pritaikytosios ir standartizuotosios duomenų apsaugos reikalavimais;

(52) atvirojo kodo kibernetinio saugumo priemonėmis ir taikomosiomis programomis gali būti prisidedama prie didesnio atvirumo ir daromas teigiamas poveikis pramonės inovacijų veiksmingumui. Atviraisiais standartais sudaromos palankesnės sąlygos saugumo priemonių sąveikumui, o tai yra naudinga pramonės suinteresuotųjų subjektų saugumo požiūriu. Atvirojo kodo kibernetinio saugumo priemonėmis ir taikomosiomis programomis gali būti daromas sverto poveikis platesnei technologijų kūrėjų bendruomenei, sudarant galimybes tiekėjų diversifikacijai. Atvirasis kodas gali paskatinti skaidresnį su kibernetiniu saugumu susijusių priemonių tikrinimo procesą ir bendruomenės inicijuotą pažeidžiamumų nustatymo procesą. Todėl valstybės narės turėtų turėti galimybę skatinti atvirojo kodo programinės įrangos ir atvirųjų standartų naudojimą, vykdydamos politiką, susijusią su atvirųjų duomenų ir atvirojo kodo naudojimu, kad skaidrumu būtų prisidėta prie saugumo užtikrinimo. Atvirojo kodo kibernetinio saugumo priemonių diegimo ir tvaraus naudojimo skatinimo politika itin svarbi mažosioms ir vidutinėms įmonėms, patiriančioms dideles įgyvendinimo sąnaudas, kurias būtų galima minimizuoti sumažinant poreikį naudoti konkrečias taikomąsias programas ar priemones;

(53) komunalinės paslaugos miestuose vis dažniau prijungiamos prie skaitmeninių tinklų, siekiant patobulinti miesto transporto tinklus, modernizuoti vandens tiekimo ir atliekų šalinimo įrenginius ir padidinti apšvietimo bei pastatų šildymo efektyvumą. Toms suskaitmenintoms komunalinėms paslaugoms kyla kibernetinių išpuolių rizika ir sėkmingo kibernetinio išpuolio atveju kyla pavojus, kad dėl jų tarpusavio sąsajų bus padaryta didelė žala piliečiams. Valstybės narės turėtų parengti politiką, pagal kurią būtų sprendžiami tokių sujungtų ar pažangiųjų miestų plėtros ir galimo jų poveikio visuomenei klausimai, esančią jų nacionalinės kibernetinio saugumo strategijos dalimi;

(54) pastaraisiais metais Sąjungoje eksponentiškai padaugėjo išpuolių naudojant išpirkos reikalavimo programinę įrangą, per kuriuos kenkimo programinė įranga užšifruoja duomenis bei sistemas ir reikalauja išpirkos už iššifravimą. Vis dažnesnius ir rimtesnius išpuolius naudojant išpirkos reikalavimo programinę įrangą gali lemti keli veiksniai, pavyzdžiui, skirtingi išpuolių modeliai, nusikalstamo verslo modeliai, susiję su „paslaugine išpirkos reikalavimo programine įranga“ ir kriptovaliuta, išpirkos reikalavimai ir išaugę išpuoliai tiekimo grandinėje. Valstybės narės turėtų parengti kovos su dažnėjančiais išpuoliais naudojant išpirkos reikalavimo programinę įrangą politiką, esančią jų nacionalinės kibernetinio saugumo strategijos dalimi;

(55) viešojo ir privačiojo sektorių partnerystė kibernetinio saugumo srityje gali būti tinkama keitimosi žiniomis, dalijimosi geriausios praktikos pavyzdžiais ir bendro supratimo tarp suinteresuotųjų subjektų nustatymo sistema. Valstybės narės turėtų skatinti politiką, pagal kurią būtų kuriamos konkrečiai su kibernetiniu saugumu susijusios viešojo ir privačiojo sektorių partnerystės. Toje politikoje, *inter alia*, turėtų būti patikslinama taikymo sritis ir dalyvaujantys suinteresuotieji subjektai, valdymo modelis, turimos finansavimo galimybės ir dalyvaujančių suinteresuotųjų subjektų tarpusavio ryšys, kiek tai susiję su viešojo ir privačiojo sektorių partnerystėmis. Viešojo ir privačiojo sektorių partnerystės gali naudotis privačiojo sektoriaus subjektų ekspertinėmis žiniomis, kad padėtų kompetentingoms institucijoms kurti pažangiausias paslaugas ir procesus, įskaitant keitimąsi informacija, ankstyvuosius perspėjimus, kibernetinių grėsmių ir incidentų valdymo pratybas, krizių valdymą ir atsparumo planavimą;

(56) savo nacionalinėse kibernetinio saugumo strategijose valstybės narės turėtų atsižvelgti į konkrečius mažųjų ir vidutinių įmonių kibernetinio saugumo poreikius. Mažosios ir vidutinės įmonės Sąjungoje sudaro didelę pramoninės ir verslo rinkos procentinę dalį ir dažnai joms sunku prisitaikyti prie naujos verslo praktikos labiau susietame pasaulyje, ir prie skaitmeninės aplinkos, kai darbuotojai dirba iš namų, o verslas vis dažniau vykdomas internetu. Kai kurios mažosios ir vidutinės įmonės susiduria su konkrečiomis kibernetinio saugumo problemomis, pvz., mažu kibernetiniu sąmoningumu, nuotolinio IT saugumo trūkumu, didelėmis kibernetinio saugumo sprendimų sąnaudomis ir išaugusiu grėsmių lygiu, pvz., išpirkos reikalavimo programinės įrangos grėsme, kurių klausimu jos turėtų gauti gaires ir pagalbą. Mažosios ir vidutinės įmonės vis dažniau tampa išpuolių prieš tiekimo grandines taikiniu dėl ne tokių griežtų jų kibernetinio saugumo rizikos valdymo priemonių ir išpuolių valdymo ir dėl to, kad turi ribotus saugumo išteklius. Tokie išpuoliai prieš tiekimo grandines daro poveikį ne tik mažosioms ir vidutinėms įmonėms ir jų veiklai atskirai, bet ir gali daryti pakopinį poveikį didesniems išpuoliams prieš subjektus, kuriems jos tiekė prekes. Valstybės narės savo nacionalinėmis kibernetinio saugumo strategijomis turėtų padėti

mažosioms ir vidutinėms įmonėms spręsti problemas, su kuriomis jos susiduria savo tiekimo grandinėse. Valstybės narės turėtų turėti nacionalinį arba regioninį kontaktinį punktą, skirtą mažosioms ir vidutinėms įmonėms, kuris teiktų gaires ir pagalbą mažosioms ir vidutinėms įmonėms arba nukreiptų jas į atitinkamas įstaigas, teikiančias gaires ir pagalbą su kibernetiniu saugumu susijusiais klausimais. Valstybės narės taip pat skatinamos siūlyti tokias paslaugas, kaip interneto svetainių konfigūravimas ir registravimo galimybių suteikimas, tokių gebėjimų neturinčioms labai mažoms ir mažosioms įmonėms;

(57) valstybės narės turėtų priimti aktyvios kibernetinės apsaugos skatinimo politiką, kaip platesnės gynybos strategijos dalį, esančią jų nacionalinių kibernetinio saugumo strategijų dalimi. Vietoj reaguojamojo pobūdžio atsako aktyvi kibernetinė apsauga yra aktyvaus pobūdžio tinklo saugumo pažeidimų prevencija, nustatymas, stebėjimas, analizė ir poveikio švelninimas, sykiu naudojant nukentėjusiųjų tinkle ir už jo ribų įdiegtus pajėgumus. Tai galėtų apimti valstybių narių siūlomas nemokamas paslaugas ar priemones, įskaitant savarankiškus pasitikrinimus, atskleidimo priemones ir turinio pašalinimo paslaugas, tam tikriems subjektams. Gebėjimas greitai ir automatiškai dalytis informacija apie grėsmes ir analize, įspėjimais apie kibernetinę veiklą ir informacija apie reagavimo veiksmus ir juos suprasti yra nepaprastai svarbus siekiant užtikrinti, kad būtų imamasi vieningų pastangų sėkmingai užkirsti kelią išpuoliams prieš tinklų ir informacines sistemas, juos atskleisti, kovoti su jais ir juos blokuoti. Aktyvi kibernetinė apsauga grindžiama gynybos strategija, į kurią neįtraukiamos puolamosios priemonės;

(58) kadangi pasinaudojimas tinklų ir informacinių sistemų pažeidžiamumais gali sukelti rimtus sutrikimus ir žalą, greitas tokių pažeidžiamumų nustatymas ir jų ištaisymas yra svarbus veiksnys mažinant riziką. Todėl tinklų ir informacines sistemas kuriantys arba administruojantys subjektai turėtų nustatyti atitinkamas procedūras, kurias taikant būtų šalinami aptikti pažeidžiamumai. Kadangi pažeidžiamumus dažnai aptinka ir atskleidžia trečiosios šalys, IRT produktų ar IRT paslaugų gamintojas arba teikėjas taip pat turėtų nustatyti būtinas procedūras, pagal kurias iš trečiųjų šalių būtų gaunama informacija apie pažeidžiamumą. Šuo atžvilgiu tarptautiniuose standartuose ISO/IEC 30111 ir ISO/IEC 29147 pateikiamos gairės dėl pažeidžiamumų šalinimo ir atskleidimo. Siekiant sudaryti sąlygas savanoriškai pažeidžiamumų atskleidimo sistemai, ypač svarbu stiprinti koordinavimą tarp pranešimą teikiančių fizinių ir juridinių asmenų ir IRT produktų ar IRT paslaugų gamintojų arba teikėjų. Koordinuotas pažeidžiamumų atskleidimas yra struktūrinis procesas, per kurį potencialiai pažeidžiamų IRT produktų ar IRT paslaugų gamintojui arba teikėjui pranešama apie pažeidžiamumus taip, kad jam būtų sudarytos sąlygos pažeidžiamumą nustatyti ir ištaisyti prieš atskleidžiant išsamią informaciją apie pažeidžiamumus trečiosioms šalims arba visuomenei. Koordinuotas pažeidžiamumų atskleidimas taip pat turėtų apimti pranešimą teikiančio fizinio ar juridinio asmens ir potencialiai pažeidžiamų IRT produktų ar IRT paslaugų gamintojo arba teikėjo koordinavimą ištaisymo laiko ir paskelbimo apie pažeidžiamumus klausimais;

(59) Komisija, ENISA ir valstybės narės turėtų toliau skatinti derinimą su tarptautiniais standartais ir esama sektoriaus gerąją praktika kibernetinio saugumo rizikos valdymo srityje, pavyzdžiui, tiekimo grandinės saugumo vertinimų, dalijimosi informacija ir pažeidžiamumų atskleidimo srityse;

(60) valstybės narės, bendradarbiaudamos su ENISA, turėtų imtis priemonių, kad palengvintų koordinuotą pažeidžiamumų atskleidimą, nustatydamos atitinkamą nacionalinę politiką. Vykdydamos savo nacionalinę politiką, valstybės narės turėtų siekti kuo didesniu mastu reaguoti į iššūkius, su kuriais susiduria pažeidžiamumų tyrėjai, įskaitant jų galimą baudžiamosios atsakomybės riziką, laikantis nacionalinės teisės. Atsižvelgiant į tai, kad pažeidžiamumus tiriantiems fiziniams ir juridiniams asmenims kai kuriose valstybėse narėse gali kilti baudžiamosios ir civilinės atsakomybės rizika, valstybės narės raginamos priimti gaires dėl informacijos saugumo tyrėjų netraukimo baudžiamojon atsakomybėn ir atleidimo nuo civilinės atsakomybės už jų veiklą;

(61) valstybės narės turėtų paskirti vieną iš savo CSIRT koordinatore, kuri, prireikus, veiktų kaip patikima tarpininkė tarp pranešimus teikiančių fizinių ar juridinių subjektų ir IRT produktų ar IRT paslaugų gamintojų arba teikėjų, kuriems pažeidžiamumas gali daryti poveikį. Koordinatore paskirtos CSIRT užduotys turėtų apimti atitinkamų subjektų identifikavimą ir susisiekimą su jais, pranešimus apie pažeidžiamumą teikiančių fizinių ar juridinių subjektų rėmimą, derybas dėl informacijos atskleidimo terminų ir pažeidžiamumų, kurie daro poveikį keliems subjektams,

valdymą (kelių šalių koordinuotas pažeidžiamumų atskleidimas). Kai pažeidžiamumas, apie kurį pranešta, galėtų daryti didelį poveikį subjektams daugiau nei vienoje valstybėje narėje, kai tikslinga, koordinatorėmis paskirtos CSIRT turėtų bendradarbiauti CSIRT tinkle;

(62) prieiga prie teisingos ir laiku pateikiamos informacijos apie pažeidžiamumus, kurie daro poveikį IRT produktams ir IRT paslaugoms, padeda geriau valdyti kibernetinio saugumo riziką. Viešai prieinamos informacijos apie pažeidžiamumus šaltiniai yra svarbi priemonė ne tik subjektams ir jų paslaugų naudotojams, bet ir kompetentingoms institucijoms bei CSIRT. Dėl tos priežasties ENISA turėtų sukurti Europos pažeidžiamumų duomenų bazę, kurioje subjektai, nepriklausomai nuo to, ar jie patenka į šios direktyvos taikymo sritį, ir jų tinklų ir informacinių sistemų tiekėjai, taip pat kompetentingos institucijos ir CSIRT gali savanoriškai atskleisti ir registruoti viešai žinomus pažeidžiamumus, siekiant sudaryti sąlygas naudotojams imtis atitinkamų rizikos mažinimo priemonių. Tos duomenų bazės tikslas – atremti unikalius iššūkius, kurie iškyla dėl Sąjungos subjektams kylančios rizikos. Be to, ENISA turėtų nustatyti tinkamą procedūrą, susijusią su viešinimo procesu, kad subjektai turėtų laiko imtis rizikos mažinimo priemonių, susijusių su jų pažeidžiamumais, ir pradėtų taikyti pažangiąsias kibernetinio saugumo rizikos valdymo priemones, taip pat kompiuterio skaitomus duomenų rinkinius ir atitinkamas sąsajas. Siekiant skatinti pažeidžiamumų atskleidimo kultūrą, atskleidimas neturėtų pakenkti pranešančiajam fiziniam ar juridiniam asmeniui;

(63) nors panašūs pažeidžiamumų registrai arba duomenų bazės jau yra sukurti, jų prieglobą vykdo ir juos tvarko subjektai, kurie nėra įsisteigę Sąjungoje. ENISA tvarkoma Europos pažeidžiamumų duomenų bazė padėtų užtikrinti didesnį paskelbimo proceso iki viešo pažeidžiamumų atskleidimo skaidrumą ir atsparumą panašių paslaugų teikimo sutrikimo arba nutraukimo atveju. Siekdama kuo labiau išvengti veiksmų dubliavimo ir siekti papildomumo, ENISA turėtų išnagrinėti galimybę sudaryti struktūrinio bendradarbiavimo susitarimus su panašiais registrais arba duomenų bazėmis, kurie priklauso trečiųjų valstybių jurisdikcijoms. Visų pirma ENISA turėtų išnagrinėti galimybę glaudžiai bendradarbiauti su Bendros pažeidžiamumų ir rizikos (BPR) sistemos operatoriais;

(64) Bendradarbiavimo grupė turėtų remti ir palengvinti valstybių narių strateginį bendradarbiavimą ir keitimąsi informacija, taip pat didinti jų tarpusavio pasitikėjimą ir patikimumą. Bendradarbiavimo grupė turėtų kas dvejus metus patvirtinti darbo programą. Darbo programa turėtų apimti veiksmus, kurių Bendradarbiavimo grupė turi imtis, kad pasiektų savo tikslus ir įvykdytų užduotis. Pirmosios pagal šią direktyvą darbo programos patvirtinimo laikotarpis turėtų būti suderintas su paskutinės darbo programos, patvirtintos pagal Direktyvą (ES) 2016/1148, laikotarpiu, kad būtų išvengta galimų Bendradarbiavimo grupės darbo sutrikimų;

(65) rengdama gairių dokumentus, Bendradarbiavimo grupė turėtų nuosekliai išsiaiškinti nacionalinius sprendimus ir patirtį, įvertinti Bendradarbiavimo grupės rezultatų poveikį nacionaliniams požiūriams, aptarti įgyvendinimo problemas ir suformuluoti konkrečias rekomendacijas, visų pirma dėl šios direktyvos perkėlimo į nacionalinę teisę suderinimo tarp valstybių narių palengvinimo, į kurias turėtų būti atsižvelgiama geriau įgyvendinant dabartines taisykles. Bendradarbiavimo grupė taip pat galėtų apibendrinti nacionalinius sprendimus, kad būtų skatinamas kibernetinio saugumo sprendimų, taikomų kiekvienam konkrečiam sektoriui visoje Sąjungoje, suderinamumas. Tai ypač svarbu tarptautinio ar tarpvalstybinio pobūdžio sektoriams;

(66) Bendradarbiavimo grupė turėtų išlikti lanksčiu forumu ir sugebėti reaguoti į kintančius ir naujus politikos prioritetus bei problemas ir kartu atsižvelgti į prieinamus išteklius. Ji galėtų nuolat rengti bendrus susitikimus su atitinkamais privačiais suinteresuotaisiais subjektais iš visos Sąjungos, kad aptartų Bendradarbiavimo grupės vykdomą veiklą ir surinktų duomenų bei informacijos apie naujus politikos iššūkius. Be to, Bendradarbiavimo grupė turėtų reguliariai vertinti kibernetinių grėsmių ar incidentų, pavyzdžiui, susijusių su išpirkos reikalavimo programine įranga, padėtį. Siekdama didinti bendradarbiavimą Sąjungos lygmeniu, Bendradarbiavimo grupė turėtų apsvarstyti galimybę pakviesti savo veikloje dalyvauti atitinkamas kibernetinio saugumo politikos srityje veikiančias Sąjungos institucijas,

įstaigas, organus ir agentūras, pavyzdžiui, Europos Parlamentą, Europolą, Europos duomenų apsaugos valdybą, Europos Sąjungos aviacijos saugos agentūrą, įsteigtą Reglamentu (ES) 2018/1139, ir Europos Sąjungos kosmoso programos agentūrą, įsteigtą Europos Parlamento ir Tarybos reglamentu (ES) 2021/696 ([14]);

(67) kompetentingos institucijos ir CSIRT turėtų turėti galimybę dalyvauti pareigūnų iš kitų valstybių narių mainų programose specialioje sistemoje ir, kai taikytina, taikant reikiamą tokiose mainų programose dalyvaujančių pareigūnų patikimumo patikrinimą, siekiant pagerinti bendradarbiavimą ir didinti valstybių narių tarpusavio pasitikėjimą. Kompetentingos institucijos turėtų imtis būtinų priemonių, kad pareigūnai iš kitų valstybių narių galėtų veiksmingai dalyvauti priimančiosios kompetentingos institucijos arba priimančiosios CSIRT veikloje;

(68) valstybės narės turėtų prisidėti kuriant Komisijos rekomendacijoje (ES) 2017/1584 ([15]) numatytą ES reagavimo į kibernetinio saugumo krizes sistemą per esamus bendradarbiavimo tinklus, visų pirma per Europos ryšių palaikymo dėl kibernetinių krizių organizacinį tinklą (EU-CyCLONe), CSIRT tinklą ir Bendradarbiavimo grupę. EU-CyCLONe ir CSIRT tinklas turėtų bendradarbiauti remdamiesi procedūrinėmis taisyklėmis, kuriomis išsamiau apibrėžiamas tas bendradarbiavimas, ir vengti bet kokio užduočių dubliavimosi. EU-CyCLONe darbo tvarkos taisyklėse taip pat turėtų būti aptarta to tinklo veikimo tvarka, įskaitant tinklo vaidmenis, bendradarbiavimo būdus, sąveiką su kitais atitinkamais dalyviais ir dalijimosi informacija šablonus, taip pat ryšių palaikymo priemones. Siekdamos valdyti krizę Sąjungos lygmeniu, atitinkamos šalys turėtų kliautis ES integruoto politinio atsako į krizes mechanizmu, kaip nustatyta Tarybos įgyvendinimo sprendime (ES) 2018/1993 ([16]) (toliau – IPCR mechanizmas). Komisija tuo tikslu turėtų naudoti aukšto lygmens tarpsektorinį krizės koordinavimo procesą ARGUS. Jei krizė susijusi su svarbiais išorės arba bendros saugumo ir gynybos politikos aspektais, turėtų būti panaudotas Europos išorės veiksmų tarnybos reagavimo į krizę mechanizmas;

(69) pagal Rekomendacijos (ES) 2017/1584 priedą didelio masto kibernetinio saugumo incidentas turėtų reikšti incidentą, į kurio sukeltą sutrikimą viena valstybė narė nepajėgia reaguoti arba kuris turi didelį poveikį ne mažiau kaip dviem valstybėms narėms. Priklausomai nuo jų priežasties ir poveikio, didelio masto kibernetinio saugumo incidentai gali stiprėti ir virsti plataus masto krizėmis, dėl kurių vidaus rinka negali tinkamai veikti, arba kelti rimtą pavojų visuomenės saugumui ir subjektų ar piliečių saugai keliose valstybėse narėse arba visoje Sąjungoje. Atsižvelgiant į tai, kad tokie incidentai yra labai įvairaus masto ir dažniausiai tarpvalstybinio pobūdžio, valstybės narės ir atitinkamos Sąjungos institucijos, įstaigos, organai ir agentūros turėtų bendradarbiauti techniniu, operatyviniu ir politiniu lygmenimis, kad tinkamai koordinuotų atsaką visoje Sąjungoje;

(70) kilus didelio masto kibernetinio saugumo incidentams ir krizėms Sąjungos lygmeniu, dėl didelės sektorių ir valstybių narių tarpusavio priklausomybės reikia imtis koordinuotų veiksmų, kad būtų užtikrintas greitas ir veiksmingas reagavimas. Siekiant užtikrinti Sąjungos saugumą ir apsaugoti jos piliečius, įmones bei institucijas nuo incidentų ir kibernetinių grėsmių, taip pat didinti asmenų ir organizacijų pasitikėjimą Sąjungos gebėjimu propaguoti ir apsaugoti pasaulinę, atvirą, laisvą, stabilią ir saugią kibernetinę erdvę, grindžiamą žmogaus teisėmis, pagrindinėmis laisvėmis, demokratija ir teisine valstybe, nepaprastai svarbu turėti kibernetinėms grėsmėms atsparias tinklų ir informacines sistemas bei prieinamus, konfidencialius ir vientisus duomenis;

([14]) 2021 m. balandžio 28 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/696, kuriuo sudaroma Sąjungos kosmoso programa, įsteigiama Europos Sąjungos kosmoso programos agentūra ir panaikinami reglamentai (ES) Nr. 912/2010, (ES) Nr. 1285/2013 bei (ES) Nr. 377/2014 ir Sprendimas Nr. 541/2014/ES (OL L 170, 2021 5 12, p. 69).

([15]) 2017 m. rugsėjo 13 d. Komisijos rekomendacija (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes (OL L 239, 2017 9 19, p. 36).

([16]) 2018 m. gruodžio 11 d. Tarybos įgyvendinimo sprendimas (ES) 2018/1993 dėl ES integruoto politinio atsako į krizes mechanizmo (OL L 320, 2018 12 17, p. 28).

(71) didelio masto kibernetinio saugumo incidentų ir krizių metu EU-CyCLONe turėtų veikti kaip tarpininkas tarp techninio ir politinio lygmens ir turėtų stiprinti bendradarbiavimą operatyviniu lygmeniu bei remti sprendimų priėmimą politiniu lygmeniu. Bendradarbiaudamas su Komisija ir atsižvelgdamas į Komisijos kompetenciją krizių valdymo srityje, EU-CyCLONe turėtų remtis CSIRT tinklo nustatytais faktais ir naudotis savo pajėgumais, kad parengtų didelio masto kibernetinio saugumo incidentų ir krizių poveikio analizę;

(72) kibernetiniai išpuoliai yra tarpvalstybinio pobūdžio ir didelis incidentas gali sutrikdyti ypatingos svarbos informacinės infrastruktūros, nuo kurios priklauso sklandus vidaus rinkos veikimas, veiklą ir jai gali būti pakenkta. Rekomendacijoje (ES) 2017/1584 aptariamas visų susijusių veikėjų vaidmuo. Be to, pagal Sąjungos civilinės saugos mechanizmo, sukurto Europos Parlamento ir Tarybos sprendimu Nr. 1313/2013/ES ([17]), Komisija yra atsakinga už bendruosius pasirengimo veiksmus, įskaitant Reagavimo į nelaimes koordinavimo centro ir Bendros ekstremaliųjų situacijų ryšių ir informacijos sistemos valdymą, informuotumo apie padėtį ir jos analizės pajėgumų išlaikymą bei tolesnį plėtojimą, taip pat pajėgumų mobilizuoti ir siųsti ekspertų grupes valstybei narei arba trečiajai valstybei paprašius pagalbos sukūrimą ir valdymą. Komisija yra atsakinga ir už analitinių ataskaitų dėl IPCR mechanizmo pagal Įgyvendinimo sprendimą (ES) 2018/1993 teikimą, be kita ko, kiek tai susiję su informuotumu apie kibernetinio saugumo padėtį ir pasirengimu, taip pat dėl informuotumo apie padėtį ir reagavimo į krizes žemės ūkio, nepalankių oro sąlygų, konfliktų kartografavimo ir prognozių, ankstyvojo perspėjimo apie gaivalines nelaimes sistemų, ekstremaliųjų sveikatos situacijų, infekcinių ligų stebėjimo, augalų sveikatos, cheminių incidentų, maisto ir pašarų saugos, gyvūnų sveikatos, migracijos, muitinės, branduolinių ir radiologinių ekstremaliųjų situacijų bei energetikos srityse;

(73) pagal SESV 218 straipsnį Sąjunga, kai tinkama, gali sudaryti tarptautinius susitarimus su trečiosiomis valstybėmis ar tarptautinėmis organizacijomis, pagal kuriuos joms būtų leidžiama dalyvauti tam tikroje Bendradarbiavimo grupės, CSIRT tinklo ir EU-CyCLONe veikloje ir toks dalyvavimas būtų organizuojamas. Tokiuose susitarimuose turėtų būti užtikrinami Sąjungos interesai ir tinkama duomenų apsauga. Tai neturėtų daryti poveikio valstybių narių teisei bendradarbiauti su trečiosiomis valstybėmis pažeidžiamumų valdymo ir kibernetinio saugumo rizikos valdymo klausimais, palengvinant pranešimų teikimą ir keitimąsi bendrąja informacija laikantis Sąjungos teisės;

(74) siekdamos palengvinti šios direktyvos veiksmingą įgyvendinimą dėl, *inter alia*, pažeidžiamumų valdymo, kibernetinio saugumo rizikos valdymo priemonių, pareigų pranešti ir dalijimosi kibernetinio saugumo informacija susitarimų, valstybės narės gali bendradarbiauti su trečiosiomis valstybėmis ir imtis veiklos, kuri laikoma tinkama tam tikslui, įskaitant keitimąsi informacija apie kibernetines grėsmes, incidentus, pažeidžiamumus, priemones ir metodus, taktiką, metodiką ir procedūras, kibernetinio saugumo krizių valdymo parengtį ir pratybas, mokymus, pasitikėjimo stiprinimą ir struktūrizuoto dalijimosi informacija susitarimus;

(75) turėtų būti įvesti tarpusavio vertinimai siekiant padėti pasimokyti iš bendros patirties, stiprinti tarpusavio pasitikėjimą ir pasiekti aukštą bendrą kibernetinio saugumo lygį. Tarpusavio vertinimai gali padėti gauti vertingų įžvalgų ir rekomendacijų, kuriomis būtų stiprinami bendri kibernetinio saugumo pajėgumai, sukuriant dar vieną funkcionalų būdą dalytis valstybių narių geriausios praktikos pavyzdžiais ir prisidedant prie valstybių narių brandos kibernetinio saugumo srityje lygio didinimo. Be to, atliekant tarpusavio vertinimus turėtų būti atsižvelgiama į panašių mechanizmų, pavyzdžiui, CSIRT tinklo tarpusavio vertinimo sistemos, rezultatus ir jais turėtų būti kuriama pridėtinė vertė bei vengiama dubliavimo. Tarpusavio vertinimų įgyvendinimas neturėtų daryti poveikio Sąjungos ar nacionalinei teisei dėl konfidencialios ar įslaptintos informacijos apsaugos;

(76) Bendradarbiavimo grupė turėtų nustatyti valstybėms narėms skirtą įsivertinimo metodiką, kuria būtų siekiama apimti tokius veiksnius kaip kibernetinio saugumo rizikos valdymo priemonių ir pareigų pranešti įgyvendinimo lygis, pajėgumų lygis ir kompetentingų institucijų užduočių vykdymo veiksmingumas, CSIRT operaciniai pajėgumai, savitarpio pagalbos įgyvendinimo lygis, dalijimosi kibernetinio saugumo informacija susitarimų įgyvendinimo lygis arba konkretūs tarpvalstybinio ar tarpsektorinio pobūdžio klausimai. Valstybės narės turėtų būti skatinamos reguliariai atlikti įsivertinimus ir Bendradarbiavimo grupėje pristatyti bei aptarti savo įsivertinimo rezultatus;

([17]) 2013 m. gruodžio 17 d. Europos Parlamento ir Tarybos sprendimas Nr. 1313/2013/ES dėl Sąjungos civilinės saugos mechanizmo (OL L 347, 2013 12 20, p. 924).

(77) atsakomybė už tinklų ir informacinių sistemų saugumo užtikrinimą didžiąja dalimi tenka esminiams ir svarbiems subjektams. Turėtų būti skatinama ir plėtojama rizikos valdymo kultūra, apimanti rizikos vertinimus ir rizikas, su kuriomis susiduriama, atitinkančių kibernetinio saugumo rizikos valdymo priemonių įgyvendinimą;

(78) kibernetinio saugumo rizikos valdymo priemonėse turėtų būti atsižvelgiama į esminio ar svarbaus subjekto priklausomybę nuo tinklų ir informacinių sistemų ir jos turėtų apimti priemones, skirtas incidentų rizikai nustatyti, incidentų prevencijos, atskleidimo, nustatymo, reagavimo į juos bei veiklos atstatymo po jų ir jų poveikio švelninimo priemones. Tinklų ir informacinių sistemų saugumas turėtų apimti saugomų, perduodamų ir tvarkomų duomenų saugumą. Kibernetinio saugumo rizikos valdymo priemonėse turėtų būti numatyta sisteminė analizė, atsižvelgiant į žmogiškąjį veiksnį, kad būtų galima susidaryti visapusišką tinklų ir informacinės sistemos saugumo vaizdą;

(79) kadangi grėsmė tinklų ir informacinių sistemų saugumui gali būti įvairios kilmės, kibernetinio saugumo rizikos valdymo priemonės turėtų būti grindžiamos visų rūšių pavojus apimančiu požiūriu, kuriuo siekiama apsaugoti tinklų ir informacines sistemas bei jų fizinę aplinką nuo tokių įvykių kaip vagystė, gaisras, potvynis, telekomunikacijų ar elektros energijos tiekimo triktys, arba nuo neleistinos fizinės prieigos prie esminio ar svarbaus subjekto informacijos ir informacijos tvarkymo objektų ir žalos jiems, ir jų trikdžių, kurie galėtų kelti pavojų saugomų, perduodamų ar tvarkomų duomenų arba per tinklų ir informacines sistemas teikiamų ar prieinamų paslaugų prieinamumui, autentiškumui, vientisumui arba konfidencialumui. Todėl kibernetinio saugumo rizikos valdymo priemonėmis taip pat turėtų būti sprendžiamas tinklų ir informacinių sistemų fizinis ir aplinkos saugumas, įtraukiant priemones, skirtas tokioms sistemoms apsaugoti nuo sistemos gedimų, žmogaus klaidų, piktavališkų veiksmų ar gamtos reiškinių laikantis Europos ir tarptautinių standartų, pavyzdžiui, įtrauktų į ISO/IEC 27000 seriją. Tuo atžvilgiu esminiai ir svarbūs subjektai savo kibernetinio saugumo rizikos valdymo priemonėmis turėtų taip pat užtikrinti žmogiškųjų išteklių saugumą ir įdiegti tinkamą prieigos kontrolės politiką. Tos priemonės turėtų būti suderinamos su Direktyva (ES) 2022/2557;

(80) siekdamos įrodyti atitiktį kibernetinio saugumo rizikos valdymo priemonėms ir nesant tinkamų Europos kibernetinio saugumo sertifikavimo schemų, priimtų pagal Europos Parlamento ir Tarybos reglamentą (ES) 2019/881 ([18]), valstybės narės, konsultuodamosi su Bendradarbiavimo grupe ir Europos kibernetinio saugumo sertifikavimo grupe, turėtų skatinti esminius ir svarbius subjektus naudoti atitinkamus Europos ir tarptautinius standartus arba gali reikalauti, kad subjektai naudotų sertifikuotus IRT produktus, IRT paslaugas ir IRT procesus;

(81) siekiant neužkrauti neproporcingos finansinės ir administracinės naštos esminiams ir svarbiems subjektams, kibernetinio saugumo rizikos valdymo priemonės turėtų būti proporcingos rizikai, kuri kyla atitinkamai tinklų ir informacinei sistemai, atsižvelgiant į tokių priemonių modernumą ir, kai taikytina, atitinkamus Europos bei tarptautinius standartus, taip pat jų įgyvendinimo išlaidas;

(82) kibernetinio saugumo rizikos valdymo priemonės turėtų būti proporcingos esminio ar svarbaus subjekto galimybės patirti riziką laipsniui ir visuomeniniam bei ekonominiam poveikiui, kurį sukeltų incidentas. Nustatant kibernetinio saugumo rizikos valdymo priemones, pritaikytas esminiams ir svarbiems subjektams, reikėtų tinkamai atsižvelgti į skirtingą esminiams ir svarbiems subjektams kylančią riziką, pavyzdžiui, subjekto svarbą, jo patiriamą riziką, įskaitant visuomenei kylančią riziką, subjekto dydį ir incidentų tikimybę bei jų sunkumą, be kita ko, jų socialinį ir ekonominį poveikį;

([18]) 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 15).

(83) esminiai ir svarbūs subjektai turėtų užtikrinti tinklų ir informacinių sistemų, kurias jie naudoja savo veikloje, saugumą. Tos sistemos visų pirma yra privačios tinklų ir informacinės sistemos, kurias administruoja esminių ir svarbių subjektų vidaus IT personalas arba kurių saugumą pavesta užtikrinti užsakomųjų paslaugų teikėjams. Šioje direktyvoje nustatytos kibernetinio saugumo rizikos valdymo priemonės ir pareigos pranešti turėtų būti taikomos atitinkamiems esminiams ir svarbiems subjektams, nepaisant to, ar tie subjektai savo tinklų ir informacines sistemas techniškai prižiūri patys, ar šias paslaugas užsako;

(84) atsižvelgiant į DNS paslaugų teikėjų, aukščiausio lygio domenų vardų registrų, debesijos kompiuterijos paslaugų teikėjų, duomenų centrų paslaugų teikėjų, turinio teikimo tinklo paslaugų teikėjų, valdomų paslaugų teikėjų, valdomų saugumo paslaugų teikėjų, internetinių prekyviečių, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų paslaugų teikėjų ir patikimumo užtikrinimo paslaugų teikėjų tarpvalstybinį pobūdį, jiems turėtų būti taikomas didesnio lygio suderinimas Sąjungos lygmeniu. Todėl kibernetinio saugumo rizikos valdymo priemonių įgyvendinimą tų subjektų atžvilgiu turėtų palengvinti įgyvendinimo aktas;

(85) rizikų, kylančių subjekto tiekimo grandinėje ir jo santykiuose su tiekėjais, pavyzdžiui, duomenų saugojimo ir tvarkymo paslaugų teikėjais arba valdomų saugumo paslaugų teikėjais ir programinės įrangos redaktoriais, mažinimas yra ypač svarbus atsižvelgiant į incidentų paplitimą tais atvejais, kai subjektai tapo kibernetinių išpuolių aukomis ir kai piktavališki nusikalstamos veikos vykdytojai galėjo kelti pavojų subjekto tinklų ir informacinių sistemų saugumui pasinaudodami pažeidžiamumais, darančiais poveikį trečiųjų šalių produktams ir paslaugoms. Todėl esminiai ir svarbūs subjektai turėtų įvertinti ir atsižvelgti į bendrą produktų ir paslaugų kokybę ir atsparumą, juose integruotas kibernetinio saugumo rizikos valdymo priemones bei savo tiekėjų ir paslaugų teikėjų kibernetinio saugumo praktiką, įskaitant jų saugaus kūrimo procedūras. Esminiai ir svarbūs subjektai visų pirma turėtų būti skatinami įtraukti kibernetinio saugumo rizikos valdymo priemones į susitarimus su savo tiesioginiais tiekėjais ir paslaugų teikėjais. Tie subjektai galėtų atsižvelgti į rizikas, kylančias dėl kitų lygmenų tiekėjų ir paslaugų teikėjų;

(86) kalbant apie paslaugų teikėjus, valdomų saugumo paslaugų teikėjai tokiose srityse kaip reagavimas į incidentus, skverbimosi testavimas, saugumo auditai ir konsultacijos atlieka itin svarbų vaidmenį padėdami subjektams užkirsti kelią incidentams, juos atskleisti, į juos reaguoti ar atstatyti po jų veiklą. Tačiau valdomų saugumo paslaugų teikėjai patys yra kibernetinių išpuolių taikiniai ir dėl jų glaudžios integracijos į subjektų veiklą kyla specifinė rizika. Todėl esminiai ir svarbūs subjektai, atrinkdami valdomų saugumo paslaugų teikėją, turėtų veikti atidžiau;

(87) kompetentingoms institucijoms vykdant jų priežiūros užduotis taip pat gali būti naudingos kibernetinio saugumo paslaugos, pavyzdžiui, saugumo auditai, skverbimosi testavimas arba reagavimas į incidentus;

(88) esminiai ir svarbūs subjektai taip pat turėtų mažinti riziką, kylančią dėl jų sąveikos ir santykių su kitais suinteresuotaisiais subjektais platesnėje ekosistemoje, be kita ko, atsižvelgiant į kovą su pramoniniu šnipinėjimu ir komercinių paslapčių apsaugą. Visų pirma tie subjektai turėtų imtis tinkamų priemonių siekdami užtikrinti, kad jų bendradarbiavimas su akademinėmis ir mokslinių tyrimų įstaigomis vyktų laikantis jų kibernetinio saugumo politikos ir būtų laikomasi gerosios praktikos, susijusios su saugia prieiga prie informacijos ir jos sklaida apskritai ir ypač su intelektinės nuosavybės apsauga. Be to, atsižvelgiant į duomenų svarbą ir vertę esminių ir svarbių subjektų veiklai, kai jie naudojasi duomenų transformavimo ir duomenų analizės paslaugomis, kurias teikia trečiosios šalys, subjektai turėtų imtis visų tinkamų kibernetinio saugumo rizikos valdymo priemonių;

(89) esminiai ir svarbūs subjektai turėtų naudoti platų pagrindinės kibernetinės higienos praktikos pavyzdžių spektrą, pavyzdžiui, nulinio pasitikėjimo principus, programinės įrangos atnaujinimus, prietaisų konfigūravimą, tinklo segmentavimą, tapatybės ir prieigos valdymą arba naudotojų informuotumą, rengti savo darbuotojams mokymus ir didinti informuotumą apie kibernetines grėsmes, duomenų viliojimą ar socialinės inžinerijos metodus. Be to, tie subjektai turėtų įvertinti savo kibernetinio saugumo pajėgumus ir prireikus siekti integruoti kibernetinio saugumo stiprinimo technologijas, pavyzdžiui, dirbtinį intelektą ar mašinų mokymosi sistemas, kad sustiprintų savo pajėgumus bei tinklų ir informacinių sistemų saugumą;

(90) siekiant toliau mažinti pagrindines tiekimo grandinės rizikas ir padėti esminiams ir svarbiems subjektams, vykdantiems veiklą sektoriuose, kuriems taikoma ši direktyva, tinkamai valdyti su tiekimo grandine ir tiekėjais susijusią riziką, Bendradarbiavimo grupė, bendradarbiaudama su Komisija ir ENISA ir prireikus, pasikonsultavusi su atitinkamais suinteresuotaisiais subjektais, įskaitant pramonės sektoriaus atstovus, turėtų atlikti koordinuotus ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimus, kaip jau padaryta 5G tinklų atveju pagal Komisijos rekomendaciją (ES) 2019/534 ([19]), siekiant nustatyti kiekvieno sektoriaus ypatingos svarbos IRT paslaugas, IRT sistemas ar IRT produktus, atitinkamas grėsmes ir pažeidžiamumus. Tokiuose koordinuotuose saugumo rizikos vertinimuose turėtų būti nustatytos priemonės, rizikos mažinimo planai ir geriausios praktikos pavyzdžiai šalinant kritines priklausomybes, galimus visuotinį neveikimą sukeliančius gedimo taškus, grėsmes, pažeidžiamumus ir kitus rizikos veiksnius, susijusius su tiekimo grandine, ir turėtų būti ieškoma būdų, kaip toliau skatinti esminius ir svarbius subjektus juos plačiau taikyti. Galimi netechniniai rizikos veiksniai, kaip antai nederamas trečiosios valstybės poveikis tiekėjams ir paslaugų teikėjams, visų pirma alternatyvių valdymo modelių atveju, apima paslėptus pažeidžiamumus arba užpakalines duris ir galimus sisteminius tiekimo sutrikimus, visų pirma technologinio susaistymo arba priklausomybės nuo tiekėjų atveju;

(91) atliekant koordinuotus ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimus, atsižvelgiant į atitinkamo sektoriaus ypatumus, turėtų būti atsižvelgiama tiek į techninius, tiek, kai tinkama, į netechninius veiksnius, įskaitant apibrėžtus Rekomendacijoje (ES) 2019/534, 5G tinklų kibernetinio saugumo ES koordinuotame rizikos vertinime ir ES 5G kibernetinio saugumo priemonių rinkinyje, dėl kurio susitarė Bendradarbiavimo grupė. Siekiant išsiaiškinti, kurioms tiekimo grandinėms turėtų būti taikomas koordinuotas saugumo rizikos vertinimas, turėtų būti atsižvelgta į šiuos kriterijus: i) kokiu mastu esminiai ir svarbūs subjektai naudojasi konkrečiomis ypatingos svarbos IRT paslaugomis, IRT sistemomis ar IRT produktais ir nuo jų priklauso; ii) konkrečių ypatingos svarbos IRT paslaugų, IRT sistemų ar IRT produktų svarba vykdant ypatingos svarbos arba jautrias funkcijas, įskaitant asmens duomenų tvarkymą; iii) alternatyvių IRT paslaugų, IRT sistemų ar IRT produktų prieinamumas; iv) visos IRT paslaugų, IRT sistemų ar IRT produktų tiekimo grandinės atsparumas sutrikimų atžvilgiu per jų gyvavimo ciklą ir v) atsirandančių IRT paslaugų, IRT sistemų ar IRT produktų atveju, jų galimą būsimą svarbą subjektų veiklai. Be to, ypatingas dėmesys turėtų būti skiriamas IRT paslaugoms, IRT sistemoms ar IRT produktams, kuriems taikomi konkretūs trečiųjų valstybių reikalavimai;

(92) siekiant supaprastinti viešųjų elektroninių ryšių tinklų ar viešai prieinamų elektroninių ryšių paslaugų teikėjams ir patikimumo užtikrinimo paslaugų teikėjams taikomas pareigas, susijusias su jų tinklų ir informacinių sistemų saugumu, taip pat sudaryti sąlygas tiems subjektams ir kompetentingoms institucijoms pagal atitinkamai Europos Parlamento ir Tarybos direktyvą (ES) 2018/1972 ([20]) ir Reglamentą (ES) Nr. 910/2014 pasinaudoti šioje direktyvoje nustatyta teisine sistema, įskaitant CSIRT, atsakingos už incidentų valdymą, paskyrimą, atitinkamų kompetentingų institucijų dalyvavimą Bendradarbiavimo grupės ir CSIRT tinklo veikloje, tie subjektai turėtų būti įtraukti į šios direktyvos taikymo sritį. Todėl atitinkamos Reglamento (ES) Nr. 910/2014 ir Direktyvos (ES) 2018/1972 nuostatos, susijusios su saugumo ir pranešimo reikalavimo nustatymu tų rūšių subjektams, turėtų būti panaikintos. Šioje direktyvoje nustatytos taisyklės dėl pranešimų teikimo pareigų neturėtų daryti poveikio Reglamentui (ES) 2016/679 ir Direktyvai 2002/58/EB;

(93) šioje direktyvoje nustatytos kibernetinio saugumo pareigos turėtų būti laikomos papildančiomis Reglamentu (ES) Nr. 910/2014 patikimumo užtikrinimo paslaugų teikėjams nustatytus reikalavimus. Turėtų būti reikalaujama, kad patikimumo užtikrinimo paslaugų teikėjai imtųsi visų tinkamų ir proporcingų jų paslaugoms kylančios rizikos valdymo priemonių, be kita ko, klientų ir pasikliaujančiųjų trečiųjų šalių atžvilgiu, ir pagal šią direktyvą praneštų apie incidentus. Tokios kibernetinio saugumo ir pranešimo pareigos turėtų būti taikomos ir teikiamų paslaugų fizinei apsaugai. Toliau taikomi Reglamento (ES) Nr. 910/2014 24 straipsnyje nustatyti reikalavimai kvalifikuotiems patikimumo užtikrinimo paslaugų teikėjams;

([19]) 2019 m. kovo 26 d. Komisijos rekomendacija (ES) 2019/534 dėl 5G tinklų kibernetinio saugumo (OL L 88, 2019 3 29, p. 42).

([20]) 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas (OL L 321, 2018 12 17, p. 36).

(94) valstybės narės atlikti patikimumo užtikrinimo paslaugų srities kompetentingų institucijų vaidmenį gali pavesti priežiūros įstaigoms pagal Reglamentą (ES) Nr. 910/2014, kad būtų užtikrintas dabartinės praktikos tęstinumas ir toliau plėtojamos taikant tą reglamentą įgytos žinios ir patirtis. Tokiu atveju kompetentingos institucijos pagal šią direktyvą turėtų glaudžiai ir laiku bendradarbiauti su tomis priežiūros įstaigomis, keisdamosi aktualia informacija, kad būtų užtikrinta veiksminga patikimumo užtikrinimo paslaugų teikėjų priežiūra ir užtikrinta, kad jie laikytųsi šioje direktyvoje bei Reglamente (ES) Nr. 910/2014 nustatytų reikalavimų. Kai taikytina, CSIRT ar kompetentinga institucija pagal šią direktyvą turėtų nedelsdama informuoti priežiūros įstaigą pagal Reglamentą (ES) Nr. 910/2014 apie visas dideles kibernetines grėsmes arba incidentus, darančius poveikį patikimumo užtikrinimo paslaugoms, apie kuriuos pranešta, taip pat apie visus atvejus, kai patikimumo užtikrinimo paslaugų teikėjas pažeidžia šią direktyvą. Pranešimų teikimo tikslais valstybės narės, kai taikytina, gali naudotis viena bendra prieiga, nustatyta siekiant užtikrinti bendrą automatinį pranešimą apie incidentus tiek priežiūros įstaigai pagal Reglamentą (ES) Nr. 910/2014, tiek CSIRT ar kompetentingai institucijai pagal šią direktyvą;

(95) kai tinkama ir siekiant išvengti nereikalingo trikdymo, perkeliant šią direktyvą į nacionalinę teisę turėtų būti atsižvelgiama į galiojančias nacionalines gaires, priimtas siekiant į nacionalinę teisę perkelti taisykles, susijusias su Direktyvos (ES) 2018/1972 40 ir 41 straipsniuose nustatytomis saugumo priemonėmis, taip plėtojant taikant Direktyvą (ES) 2018/1972 jau įgytas žinias ir patirtį, susijusias su saugumo priemonėmis ir pranešimais apie incidentus. ENISA taip pat gali parengti gaires dėl saugumo reikalavimų ir pareigų pranešti, skirtas viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjams, kad būtų sudarytos palankesnės sąlygos suderinimui bei pertvarkai ir kuo labiau sumažinti trikdžiai. Valstybės narės gali pagal Direktyvą (ES) 2018/1972 pavesti elektroninių ryšių srities kompetentingų institucijų vaidmenį atlikti nacionalinėms reguliavimo institucijoms, kad būtų užtikrintas dabartinės praktikos tęstinumas ir toliau plėtojamos įgyvendinant tą direktyvą įgytos žinios ir patirtis;

(96) atsižvelgiant į didėjančią su numeriu nesiejamo asmenų tarpusavio ryšio paslaugų, kaip apibrėžta Direktyvoje (ES) 2018/1972, svarbą, būtina užtikrinti, kad tokioms paslaugoms, atsižvelgiant į jų specifinį pobūdį ir ekonominę svarbą, taip pat būtų taikomi tinkami saugumo reikalavimai. Kadangi išpuolių perimetras vis didėja, su numeriu nesiejamo asmenų tarpusavio ryšio paslaugos, pavyzdžiui, pranešimų paslaugos, tampa plačiai paplitusiais išpuolių vektoriais. Piktavališki nusikalstamos veikos vykdytojai naudoja platformas, kad bendrautų su aukomis ir jas suviliotų atverti saugumui pavojų keliančius interneto puslapius, todėl padidėja incidentų, susijusių su asmens duomenų naudojimu ir atitinkamai – tinklų ir informacinių sistemų saugumu, tikimybė. Su numeriu nesiejamo asmenų tarpusavio ryšio paslaugų teikėjai turėtų užtikrinti tinklų ir informacinių sistemų saugumo lygį, atitinkantį keliamą riziką. Atsižvelgiant į tai, kad su numeriu nesiejamo asmenų tarpusavio ryšio paslaugų teikėjai paprastai neturi tikrų galimybių kontroliuoti tinklais siunčiamus perdavimo signalus, galima laikyti, kad tam tikrais atžvilgiais tokioms paslaugoms kyla mažesnio laipsnio rizika nei tradicinėms elektroninių ryšių paslaugoms. Tas pats pasakytina ir apie asmenų tarpusavio ryšio paslaugas, kaip apibrėžta Direktyvoje (ES) 2018/1972, kurias teikiant naudojami numeriai ir kurias teikiant faktiškai nekontroliuojamas signalų perdavimas;

(97) vidaus rinka labiau nei bet kada priklauso nuo interneto veikimo. Beveik visų esminių ir svarbių subjektų paslaugos priklauso nuo internetu teikiamų paslaugų. Siekiant užtikrinti sklandų esminių ir svarbių subjektų teikiamų paslaugų teikimą, svarbu, kad visi viešųjų elektroninių ryšių tinklų teikėjai įdiegtų tinkamas kibernetinio saugumo rizikos valdymo priemones ir praneštų apie su jomis susijusius didelius incidentus. Valstybės narės turėtų užtikrinti, kad būtų išlaikytas viešųjų elektroninių ryšių tinklų saugumas ir kad jų gyvybiškai svarbūs saugumo interesai būtų apsaugoti nuo sabotažo ir šnipinėjimo. Kadangi tarptautinis junglumas stiprina ir spartina konkurencingą Sąjungos ir jos ekonomikos skaitmeninimą, apie incidentus, darančius poveikį povandeniniams ryšių kabeliams, turėtų būti pranešama CSIRT arba, kai taikytina, kompetentingai institucijai. Nacionalinėje kibernetinio saugumo strategijoje, kai tinkama, turėtų būti atsižvelgiama į povandeninių ryšių kabelių kibernetinį saugumą ir į ją turėtų būti įtraukta galimos kibernetinio saugumo rizikos kartograma bei rizikos mažinimo priemonės, siekiant užtikrinti aukščiausią jų apsaugos lygį;

(98) siekiant užtikrinti viešųjų elektroninių ryšių tinklų ir viešai prieinamų elektroninių ryšių paslaugų saugumą, turėtų būti skatinama naudoti šifravimo technologijas, visų pirma ištisinį šifravimą, taip pat į duomenis orientuotas saugumo koncepcijas, pavyzdžiui, kartografiją, segmentavimą, žymėjimą, prieigos politiką ir prieigos valdymą bei automatinius sprendimus dėl prieigos. Kai būtina, šifravimo, visų pirma ištisinio šifravimo, naudojimas turėtų būti privalomas viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjams laikantis pritaikytojo ir standartizuotojo saugumo bei privatumo principų šios direktyvos tikslais. Ištisinio šifravimo naudojimas turėtų derėti su valstybių narių įgaliojimais užtikrinti savo esminių saugumo interesų apsaugą ir visuomenės saugumą ir leisti užkirsti kelią nusikalstamoms veikoms, jas tirti, nustatyti ir vykdyti baudžiamąjį persekiojimą už jas laikantis Sąjungos teisės. Tačiau dėl to neturėtų būti susilpnintas ištisinis šifravimas, kuris yra kritinė technologija siekiant veiksmingai apsaugoti duomenis ir privatumą bei ryšių saugumą;

(99) siekiant užtikrinti viešųjų elektroninių ryšių tinklų ir viešai prieinamų elektroninių ryšių paslaugų saugumą ir užkirsti kelią piktnaudžiavimui bei manipuliavimui jais, turėtų būti skatinama naudoti saugaus maršruto parinkimo standartus, kad būtų užtikrintas maršruto parinkimo funkcijų vientisumas ir patikimumas visoje prieigos prie interneto paslaugų tiekėjų ekosistemoje;

(100) siekiant apsaugoti interneto funkcionalumą ir vientisumą ir skatinti DNS saugumą bei atsparumą, atitinkami suinteresuotieji subjektai, įskaitant Sąjungos privačiojo sektoriaus subjektus, viešai prieinamų elektroninių ryšių paslaugų teikėjus, visų pirma prieigos prie interneto paslaugų teikėjus, ir interneto paieškos sistemų teikėjus, turėtų būti skatinami priimti DNS keitimo įvairinimo strategiją. Be to, valstybės narės turėtų skatinti kurti ir naudoti viešą ir saugų Europos DNS keitiklį;

(101) šia direktyva nustatomas kelių etapų pranešimų apie didelius incidentus teikimo metodas, siekiant užtikrinti tinkamą pusiausvyrą tarp, viena vertus, greito pranešimų teikimo, kuris padeda sumažinti galimą didelių incidentų plitimą ir suteikia galimybę esminiams ir svarbiems subjektams prašyti pagalbos, ir, kita vertus, išsamių pranešimų, kuriuose atsižvelgiama į vertingą su atskirais incidentais susijusią patirtį ir ilgainiui didinamas atskirų subjektų ir visų sektorių kibernetinis atsparumas. Tuo atžvilgiu šioje direktyvoje turėtų būti numatytas pranešimas apie incidentus, kurie, remiantis atitinkamo subjekto atliktu pradiniu vertinimu, galėtų sukelti didelį paslaugų teikimo sutrikdymą arba finansinių nuostolių tam subjektui arba paveiktų kitus fizinius ar juridinius asmenis sukeliant jiems didelės turtinės arba neturtinės žalos. Atliekant tokį pradinį vertinimą turėtų būti atsižvelgiama, *inter alia*, į paveiktas tinklų ir informacines sistemas, ypač į jų svarbą subjekto paslaugų teikimui, kibernetinės grėsmės rimtumą ir technines charakteristikas bei visus pagrindinius pažeidžiamumus, kuriais naudojamasi, taip pat į subjekto patirtį įvykus panašiems incidentams. Tokie rodikliai, kaip poveikio paslaugos veikimui mastas, incidento trukmė arba paveiktų paslaugų gavėjų skaičius, galėtų būti svarbūs nustatant, ar paslaugos teikimo sutrikdymas yra didelis;

(102) jei esminiai ar svarbūs subjektai sužino apie didelį incidentą, reikalaujama, kad jie nepagrįstai nedelsdami ir bet kuriuo atveju per 24 valandas pateiktų ankstyvąjį perspėjimą. Po to ankstyvojo perspėjimo turėtų būti pateikiamas pranešimas apie incidentą. Atitinkami subjektai turėtų nepagrįstai nedelsdami ir bet kuriuo atveju per 72 valandas nuo tada, kai sužinojo apie didelį incidentą, pateikti pranešimą apie incidentą, visų pirma siekdami atnaujinti ankstyvuoju perspėjimu pateiktą informaciją ir pateikti didelio incidento, įskaitant jo rimtumą ir poveikį, pradinį vertinimą, taip pat užvaldymo rodiklius, jei tokių yra. Galutinis pranešimas turėtų būti pateiktas ne vėliau kaip per vieną mėnesį nuo pranešimo apie incidentą. Ankstyvajame perspėjime turėtų būti pateikta tik ta informacija, kurios reikia, kad CSIRT arba, kai taikytina, kompetentinga institucija, būtų informuota apie didelį incidentą, o atitinkamas subjektas prireikus galėtų kreiptis pagalbos. Tokiame ankstyvajame perspėjime, jei taikytina, turėtų būti nurodyta, ar įtariama, kad didelį incidentą sukėlė neteisėti arba piktavališki veiksmai, ir ar tikėtina, kad jis turės tarpvalstybinį poveikį. Valstybės narės turėtų užtikrinti, kad dėl pareigos pateikti tą ankstyvąjį perspėjimą arba vėlesnį pranešimą apie incidentą pranešančio subjekto ištekliai nebūtų nukreipti nuo veiklos, susijusios su incidentų valdymu, kuriai turėtų būti teikiama pirmenybė, siekiant užkirsti kelią tam, kad dėl pranešimų apie incidentus teikimo pareigų nebūtų nukreipiami ištekliai nuo reagavimo į didelius incidentus valdymo arba kitaip nebūtų pakenkta subjekto

pastangoms šioje srityje. Tuo atveju, jei galutinio pranešimo pateikimo metu incidentas tebevyksta, valstybės narės turėtų užtikrinti, kad atitinkami subjektai tuo metu pateiktų pažangos ataskaitą, o galutinę ataskaitą – per vieną mėnesį nuo tada, kai suvaldė didelį incidentą;

(103) kai taikytina, esminiai ir svarbūs subjektai turėtų nedelsdami pranešti savo paslaugų gavėjams apie visas priemones ar taisomąsias priemones, kurių jie gali imtis, kad sumažintų dėl didelės kibernetinės grėsmės kylančią riziką. Kai tinkama ir ypač tais atvejais, kai tikėtina, kad didelė kibernetinė grėsmė pasireikš, tie subjektai taip pat turėtų informuoti savo paslaugų gavėjus apie pačią grėsmę. Reikalavimo informuoti tuos gavėjus apie dideles kibernetines grėsmes turėtų būti laikomasi dedant visas įmanomas pastangas, tačiau jis neturėtų atleisti tų subjektų nuo pareigos savo sąskaita imtis tinkamų ir neatidėliotinų priemonių, kad būtų užkirstas kelias tokioms grėsmėms arba jos būtų pašalintos ir atkurtas įprastas paslaugos saugumo lygis. Tokia informacija apie dideles kibernetines grėsmes paslaugų gavėjams turėtų būti teikiama nemokamai ir parengta lengvai suprantama kalba;

(104) viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai turėtų įgyvendinti pritaikytojo ir standartizuotojo saugumo priemones ir informuoti savo paslaugų gavėjus apie dideles kibernetines grėsmes ir priemones, kurių jie gali imtis savo prietaisų ir ryšių saugumui užtikrinti, pavyzdžiui, naudodami konkrečių rūšių programinę įrangą arba šifravimo technologijas;

(105) iniciatyvus požiūris į kibernetines grėsmes yra nepaprastai svarbus kibernetinio saugumo rizikos valdymo priemonių elementas, kuris turėtų sudaryti sąlygas kompetentingoms institucijoms veiksmingai užkirsti kelią kibernetinių grėsmių tapimui incidentais, dėl kurių gali būti patiriama didelė turtinė ar neturtinė žala. Tuo tikslu labai svarbu, kad apie kibernetines grėsmes būtų pranešama. Todėl subjektai raginami savanoriškai pranešti apie kibernetines grėsmes;

(106) siekiant supaprastinti pagal šią direktyvą reikalaujamą informacijos pranešimą ir sumažinti subjektams tenkančią administracinę naštą, valstybės narės turėtų numatyti technines priemones, pavyzdžiui, vieną bendrą prieigą, automatizuotas sistemas, internetines formas, patogias naudoti sąsajas, šablonus, specialias platformas, skirtas subjektams naudoti, nepriklausomai nuo to, ar jie patenka į šios direktyvos taikymo sritį, kad būtų galima teikti atitinkamą su pranešimų teikimu susijusią informaciją. Sąjungos finansavimas, kuriuo remiamas šios direktyvos įgyvendinimas, visų pirma pagal Skaitmeninės Europos programą, nustatytą Europos Parlamento ir Tarybos reglamentu (ES) 2021/694 ([21]), galėtų apimti paramą vienai bendrai prieigai. Be to, subjektai dažnai atsiduria tokioje padėtyje, kai apie konkretų incidentą dėl jo ypatumų, atsižvelgiant į įvairiuose teisės aktuose nustatytas pareigas pranešti, reikia pranešti įvairioms institucijoms. Tokiais atvejais sukuriama papildoma administracinė našta ir gali kilti neaiškumų dėl tokių pranešimų formos ir procedūrų. Tais atvejais, kai įsteigiama viena bendra prieiga, valstybės narės taip pat raginamos tą vieną bendrą prieigą naudoti pranešimams apie saugumo incidentus, kurių reikalaujama pagal kitus Sąjungos teisės aktus, pavyzdžiui, Reglamentą (ES) 2016/679 ir Direktyvą 2002/58/EB, teikti. Tokios vienos bendros prieigos naudojimas pranešimams apie saugumo incidentus teikti pagal Reglamentą (ES) 2016/679 ir Direktyvą 2002/58/EB neturėtų daryti poveikio Reglamento (ES) 2016/679 ir Direktyvos 2002/58/EB nuostatų, visų pirma susijusių su juose nurodytų institucijų nepriklausomumu, taikymui. ENISA, bendradarbiaudama su Bendradarbiavimo grupe, turėtų parengti bendrus pranešimo šablonus, pateikdama gaires, kuriomis supaprastinama ir racionalizuojama pagal Sąjungos teisę reikalaujama pranešimų teikimo informacija ir sumažinama pranešantiems subjektams tenkanti administracinė našta;

(107) kai įtariama, kad incidentas yra susijęs su sunkia nusikalstama veika pagal Sąjungos arba nacionalinę teisę, valstybės narės turėtų skatinti esminius ir svarbius subjektus, remiantis pagal Sąjungos teisę taikytinomis baudžiamojo proceso taisyklėmis, pranešti atitinkamoms teisėsaugos institucijoms apie įtariamus sunkius nusikalstamo pobūdžio incidentus. Atitinkamais atvejais, nedarant poveikio Europolui taikomų asmens duomenų apsaugos taisyklėms, pageidautina, kad skirtingų valstybių narių kompetentingų institucijų ir teisėsaugos institucijų veiklos koordinavimą palengvintų Europos kovos su elektroniniu nusikalstamumu centras (EC3) ir ENISA;

([21]) 2021 m. balandžio 29 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/694, kuriuo nustatoma Skaitmeninės Europos programa ir panaikinamas Sprendimas (ES) 2015/2240 (OL L 166, 2021 5 11, p. 1).

(108) daugeliu atvejų dėl incidentų kyla pavojus asmens duomenų saugumui. Tokiomis aplinkybėmis kompetentingos institucijos turėtų bendradarbiauti ir keistis informacija visais svarbiais klausimais su institucijomis, nurodytomis Reglamente (ES) 2016/679 ir Direktyvoje 2002/58/EB;

(109) siekiant užtikrinti DNS saugumą, stabilumą ir atsparumą, būtina turėti tikslias ir išsamias domenų vardų registracijos duomenų (WHOIS duomenų) bazes ir suteikti teisėtą prieigą prie tokių duomenų, o tai savo ruožtu prisideda prie aukšto bendro kibernetinio saugumo lygio visoje Sąjungoje. Tuo konkrečiu tikslu turėtų būti reikalaujama, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai tvarkytų tam tikrus duomenis, būtinus tam tikslui pasiekti. Toks tvarkymas turėtų būti laikomas teisine prievole, kaip tai suprantama Reglamento (ES) 2016/679 6 straipsnio 1 dalies c punkte. Ta prievole nedaromas poveikis galimybei domenų vardų registracijos duomenis rinkti kitais tikslais, pavyzdžiui, remiantis sutartimi arba teisiniais reikalavimais, nustatytais kitoje Sąjungos ar nacionalinėje teisėje. Tos prievolės tikslas – užtikrinti išsamų tikslių registracijos duomenų rinkinį ir dėl jos tie patys duomenys neturėtų būti renkami kelis kartus. Aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai turėtų bendradarbiauti tarpusavyje, kad būtų išvengta tos užduoties dubliavimosi;

(110) siekiant užkirsti kelią piktnaudžiavimui DNS ir kovoti su juo, taip pat užkirsti kelią incidentams ir juos atskleisti bei į juos reaguoti, labai svarbu teisėtiems prieigos prašantiems subjektams užtikrinti domenų vardų registracijos duomenų prieinamumą ir galimybę laiku su jais susipažinti. Teisėti prieigos prašantys subjektai turi būti suprantami kaip bet kuris fizinis ar juridinis asmuo, teikiantis prašymą pagal Sąjungos arba nacionalinę teisę. Jie gali apimti institucijas, kurios yra kompetentingos pagal šią direktyvą ir kurios yra kompetentingos pagal Sąjungos ar nacionalinę teisę nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas srityje, taip pat CERT arba CSIRT. Pagal Sąjungos ir nacionalinę teisę turėtų būti reikalaujama, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai suteiktų teisėtiems prieigos prašantiems subjektams teisėtą prieigą prie konkrečių domenų vardų registracijos duomenų, kurie yra būtini prieigos prašymo tikslais. Prie teisėtų prieigos prašančių subjektų prašymo turėtų būti pridėtas motyvų pareiškimas, kuriuo remiantis būtų galima įvertinti prieigos prie duomenų būtinumą;

(111) siekiant užtikrinti tikslių ir išsamių domenų vardų registracijos duomenų prieinamumą, aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai turėtų rinkti domenų vardų registracijos duomenis ir užtikrinti jų vientisumą ir prieinamumą. Visų pirma, aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai turėtų nustatyti politiką ir procedūras, skirtas tiksliems ir išsamiems domenų vardų registracijos duomenims rinkti ir saugoti, taip pat užkirsti kelią netiksliems registracijos duomenims ir juos ištaisyti laikantis Sąjungos duomenų apsaugos teisės. Toje politikoje ir procedūrose turėtų būti kuo labiau atsižvelgiama į standartus, kuriuos tarptautiniu lygmeniu parengė įvairių suinteresuotųjų subjektų valdymo struktūros. Aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai turėtų patvirtinti ir įgyvendinti proporcingas procedūras, kurios skirtos patikrinti domenų vardų registracijos duomenis. Tos procedūros turėtų atspindėti geriausią sektoriuje taikomą praktiką ir, kiek įmanoma, elektroninės atpažinties srityje padarytą pažangą. Tikrinimo procedūros, be kita ko, gali būti *ex ante* kontrolė, atliekama registracijos metu, ir *ex post* kontrolė, atliekama po registracijos. Aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai turėtų visų pirma patikrinti bent vieną iš susisiekimo su registruotoju būdų;

(112) turėtų būtų reikalaujama, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai viešai skelbtų domenų vardų registracijos duomenis, kuriems netaikoma Sąjungos duomenų apsaugos teisė, pavyzdžiui, duomenis, susijusius su juridiniais asmenimis, atsižvelgiant į Reglamento (ES) 2016/679 preambulę. Juridinių asmenų atveju aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai turėtų viešai skelbti bent registruotojo pavadinimą bei kontaktinį telefono numerį. Kontaktinis el. pašto adresas taip pat turėtų būti skelbiamas su sąlyga, kad jame nėra jokių asmens duomenų, kaip, pavyzdžiui, el. pašto slapyvardžių ar funkcinių paskyrų atveju. Pagal Sąjungos duomenų apsaugos teisę aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys domenų vardų registravimo paslaugas, taip pat turėtų suteikti teisėtiems prieigos prašantiems subjektams teisėtą prieigą prie konkrečių domenų vardų registracijos duomenų, susijusių su fiziniais asmenimis. Valstybės narės turėtų reikalauti, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai nepagrįstai nedelsdami atsakytų į teisėtų prieigos prašančių subjektų prašymus atskleisti domenų vardų registracijos duomenis. Aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys domenų vardų registravimo paslaugas, turėtų nustatyti registracijos duomenų skelbimo ir atskleidimo politiką ir procedūras, įskaitant susitarimus dėl paslaugų lygio, skirtus nagrinėti teisėtų prieigos prašančių subjektų prašymus suteikti prieigą. Toje politikoje ir procedūrose turėtų būti kuo labiau

atsižvelgiama į bet kokias gaires ir standartus, kuriuos tarptautiniu lygmeniu parengė įvairių suinteresuotųjų subjektų valdymo struktūros. Prieigos procedūra galėtų apimti sąsajos, portalo ar kitos techninės priemonės naudojimą, kad būtų sukurta veiksminga registracijos duomenų prašymų ir prieigos prie jų sistema. Siekdama skatinti suderintą praktiką visoje vidaus rinkoje, Komisija gali, nedarant poveikio Europos duomenų apsaugos valdybos kompetencijai, pateikti tokių procedūrų gaires, kuriose kuo labiau atsižvelgiama į įvairių suinteresuotųjų subjektų valdymo struktūrų tarptautiniu lygmeniu parengtus standartus. Valstybės narės turėtų užtikrinti, kad visų rūšių prieiga prie asmens ir ne asmens domenų vardų registracijos duomenų būtų nemokama;

(113) subjektai, kuriems taikoma ši direktyva, turėtų būti laikomi priklausančiais valstybės narės, kurioje jie įsisteigę, jurisdikcijai. Tačiau viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai turėtų būti laikomi priklausančiais valstybės narės, kurioje jie teikia savo paslaugas, jurisdikcijai. DNS paslaugų teikėjai, aukščiausio lygio domenų vardų registrai, domenų vardų registravimo paslaugas teikiantys subjektai, debesijos kompiuterijos paslaugų teikėjai, duomenų centrų paslaugų teikėjai, turinio teikimo tinklo paslaugų teikėjai, valdomų paslaugų teikėjai, valdomų saugumo paslaugų teikėjai, taip pat internetinių prekyviečių, interneto paieškos sistemų bei socialinio tinklo paslaugų platformų paslaugų teikėjai turėtų būti laikomi priklausančiais valstybės narės, kurioje yra jų pagrindinė buveinė Sąjungoje, jurisdikcijai. Viešojo administravimo subjektai turėtų priklausyti valstybės narės, kuri juos įsteigė, jurisdikcijai. Jeigu subjektas teikia paslaugas arba yra įsisteigęs daugiau nei vienoje valstybėje narėje, jis turėtų priklausyti atskirai ir konkuruojančiai kiekvienos iš tų valstybių narių jurisdikcijai. Tų valstybių narių kompetentingos institucijos turėtų bendradarbiauti, teikti viena kitai savitarpio pagalbą ir prireikus vykdyti bendrus priežiūros veiksmus. Tuo atveju, kai valstybės narės naudojasi jurisdikcija, jos neturėtų taikyti vykdymo užtikrinimo priemonių ar sankcijų daugiau kaip vieną kartą už tą patį elgesį, laikydamosi ne *bis in idem* principo;

(114) siekiant atsižvelgti į DNS paslaugų teikėjų, aukščiausio lygio domenų vardų registrų, domenų vardų registravimo paslaugas teikiančių subjektų, debesijos kompiuterijos paslaugų teikėjų, duomenų centrų paslaugų teikėjų, turinio teikimo tinklo paslaugų teikėjų, valdomų paslaugų teikėjų, valdomų saugumo paslaugų teikėjų, taip pat internetinių prekyviečių, interneto paieškos sistemų bei socialinio tinklo paslaugų platformų paslaugų teikėjų tarpvalstybinį paslaugų ir veiklos pobūdį, jurisdikciją tų subjektų atžvilgiu turėtų turėti tik viena valstybė narė. Jurisdikcija turėtų būti priskirta valstybei narei, kurioje yra atitinkamo subjekto pagrindinė buveinė Sąjungoje. Šioje direktyvoje įsisteigimo kriterijus reiškia veiksmingą veiklos vykdymą per nuolatines struktūras. Tuo atžvilgiu teisinė tokių struktūrų forma, nepaisant to, ar tai filialas ar patronuojamoji įmonė, turinti juridinio asmens statusą, nėra lemiamas veiksnys. Tai, ar šio kriterijaus laikomasi, neturėtų priklausyti nuo to, ar tinklų ir informacinės sistemos fiziškai yra tam tikroje vietoje; tokių sistemų buvimas ir naudojimas pats savaime nereiškia tokios pagrindinės buveinės, todėl tai nėra lemiami kriterijai, kuriais remiantis nustatoma pagrindinė buveinė. Turėtų būti laikoma, kad pagrindinė buveinė yra valstybėje narėje, kurioje Sąjungoje daugiausia priimami su kibernetinio saugumo rizikos valdymo priemonėmis susiję sprendimai. Paprastai ji sutampa su subjektų centrinės administracijos vieta Sąjungoje. Jei tokios valstybės narės neįmanoma nustatyti arba jei tokie sprendimai nepriimami Sąjungoje, turėtų būti laikoma, kad pagrindinė buveinė yra valstybėje narėje, kurioje vykdomos kibernetinio saugumo operacijos. Jei tokios valstybės narės neįmanoma nustatyti, turėtų būti laikoma, kad pagrindinė buveinė yra valstybėje narėje, kurioje subjektas turi padalinį, kuriame dirba daugiausia darbuotojų Sąjungoje. Jeigu paslaugas teikia įmonių grupė, pagrindinė kontroliuojančiosios įmonės buveinė turėtų būti laikoma pagrindine įmonių grupės buveine;

(115) kai viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjas teikia viešai prieinamą rekursinę DNS paslaugą tik kaip interneto prieigos paslaugos dalį, subjektas turėtų būti laikomas priklausančiu visų valstybių narių, kuriose teikiamos jo paslaugos, jurisdikcijai;

(116) kai paslaugas Sąjungoje siūlo DNS paslaugų teikėjas, aukščiausio lygio domenų vardų registras, domenų vardų registravimo paslaugas teikiantis subjektas, debesijos kompiuterijos paslaugų teikėjas, duomenų centrų paslaugų teikėjas, turinio teikimo tinklo paslaugų teikėjas, valdomų paslaugų teikėjas, valdomų saugumo paslaugų teikėjas arba internetinės prekyvietės, interneto paieškos sistemos ar socialinio tinklo paslaugų platformos paslaugų teikėjas, kuris nėra įsisteigęs Sąjungoje, jis turėtų paskirti atstovą Sąjungoje. Siekiant nustatyti, ar toks subjektas siūlo paslaugas Sąjungoje, reikėtų įvertinti, ar subjektas ketina siūlyti paslaugas asmenims vienoje ar daugiau valstybių narių. Turėtų būti laikoma, kad vien to, jog Sąjungoje prieinama subjekto ar tarpininko interneto svetainė arba el. pašto adresas ar kiti kontaktiniai duomenys arba kad vartojama kalba, kuri paprastai vartojama trečiojoje valstybėje, kurioje yra įsisteigęs subjektas, nepakanka siekiant įrodyti, kad esama tokio ketinimo. Tačiau dėl tokių veiksnių kaip kalba ar valiuta, paprastai vartojamų (naudojamų) vienoje ar daugiau valstybių narių, įskaitant galimybę užsakyti paslaugas ta kalba, arba nurodant Sąjungoje esančius vartotojus ar naudotojus, gali būti akivaizdu, kad subjektas ketina siūlyti paslaugas Sąjungoje. Atstovas turėtų veikti subjekto vardu, o kompetentingos institucijos arba CSIRT turėtų turėti galimybę kreiptis į atstovą. Atstovas turėtų būti aiškiai paskirtas rašytiniu subjekto įgaliojimu veikti pastarojo vardu vykdant šioje direktyvoje nustatytas jo pareigas, įskaitant pranešimą apie incidentus;

(117) siekiant užtikrinti aiškų DNS paslaugų teikėjų, aukščiausio lygio domenų vardų registrų, domenų vardų registravimo paslaugas teikiančių subjektų, debesijos kompiuterijos paslaugų teikėjų, duomenų centrų paslaugų teikėjų, turinio teikimo tinklo paslaugų teikėjų, valdomų paslaugų teikėjų, valdomų saugumo paslaugų teikėjų, taip pat internetinių prekyviečių, interneto paieškos sistemų bei socialinio tinklo paslaugų platformų paslaugų teikėjų, kurie teikia paslaugas visoje Sąjungoje, patenkančias į šios direktyvos taikymo sritį, vaizdą, ENISA turėtų sukurti ir tvarkyti tokių subjektų registrą, remiantis iš valstybių narių gauta informacija, kai taikytina, naudojant nacionalinius mechanizmus, sukurtus subjektų saviregistracijai. Bendrieji kontaktiniai punktai turėtų perduoti ENISA informaciją ir visus jos pakeitimus. Kad būtų užtikrintas į tą registrą įtrauktinos informacijos tikslumas ir išsamumas, valstybės narės gali pateikti ENISA bet kokiuose nacionaliniuose registruose turimą informaciją apie tuos subjektus. ENISA ir valstybės narės turėtų imtis priemonių tokių registrų sąveikumui palengvinti, kartu užtikrindamos konfidencialios ar įslaptintos informacijos apsaugą. ENISA turėtų nustatyti tinkamus informacijos klasifikavimo ir valdymo protokolus, kad užtikrintų atskleistos informacijos saugumą ir konfidencialumą ir apribotų prieigą prie tokios informacijos, jos saugojimą ir perdavimą numatytiems naudotojams;

(118) jeigu pagal šią direktyvą keičiamasi informacija, kuri yra įslaptinta pagal Sąjungos arba nacionalinę teisę, apie ją pranešama arba ja kitaip dalijamasi, turėtų būti taikomos atitinkamos įslaptintos informacijos tvarkymo taisyklės. Be to, ENISA turėtų turėti infrastruktūrą, procedūras ir taisykles, kuriomis būtų tvarkoma neskelbtina ir įslaptinta informacija, laikantis ES įslaptintai informacijai apsaugoti taikomų saugumo taisyklių;

(119) kadangi kibernetinės grėsmės tampa vis sudėtingesnės ir painesnės, geros tokių grėsmių atskleidimo ir prevencijos priemonės labai priklauso nuo to, ar subjektai reguliariai keičiasi žvalgybos informacija apie grėsmes ir pažeidžiamumą. Dalijantis informacija padedama didinti informuotumą apie kibernetines grėsmes, o tai savo ruožtu didina subjektų gebėjimą užkirsti kelią tokioms grėsmėms virsti incidentais ir sudaro sąlygas subjektams geriau suvaldyti incidentų poveikį ir veiksmingiau atstatyti veiklą. Nesant gairių Sąjungos lygmeniu, atrodo, kad keli veiksniai trukdo dalytis tokia žvalgybos informacija, visų pirma netikrumas dėl suderinamumo su konkurencijos ir atsakomybės taisyklėmis;

(120) valstybės narės turėtų skatinti subjektus ir jiems padėti bendrai naudotis savo asmeninėmis žiniomis ir praktine praktika strateginiu, taktiniu ir operatyviniu lygmenimis, kad sustiprintų savo gebėjimus tinkamai užkirsti kelią incidentams, juos atskleisti, į juos reaguoti ar atstatyti po jų veiklą arba sumažinti jų poveikį. Todėl būtina sudaryti sąlygas Sąjungos lygmeniu, kad atsirastų savanoriško dalijimosi kibernetinio saugumo informacija susitarimai. Tuo tikslu valstybės narės turėtų aktyviai padėti subjektams, kaip antai tiems, kurie daugiausia dėmesio skiria kibernetinio saugumo paslaugoms ir moksliniams tyrimams, taip pat atitinkamiems subjektams, kuriems ši direktyva netaikoma, ir juos skatinti dalyvauti keičiantis kibernetinio saugumo informacija pagal tokius susitarimus. Tie susitarimai turėtų būti parengti pagal Sąjungos konkurencijos taisykles ir Sąjungos duomenų apsaugos teisės aktus;

(121) esminių ir svarbių subjektų vykdomas asmens duomenų tvarkymas tiek, kiek tai būtina ir proporcinga siekiant užtikrinti tinklų ir informacinių sistemų saugumą, galėtų būti laikomas teisėtu remiantis tuo, kad toks tvarkymas atitinka duomenų valdytojui taikomą teisinę prievolę pagal Reglamento (ES) 2016/679 6 straipsnio 1 dalies c punkto ir 6 straipsnio 3 dalies reikalavimus. Taip pat tvarkyti asmens duomenis gali reikėti siekiant teisėtų interesų, kurių siekia esminiai ir svarbūs subjektai, taip pat tų subjektų vardu veikiantys saugumo technologijų bei paslaugų tiekėjai ir teikėjai, laikantis Reglamento (ES) 2016/679 6 straipsnio 1 dalies f punkto, be kita ko, kai toks tvarkymas yra būtinas pagal dalijimosi kibernetinio saugumo informacija susitarimus arba savanoriškai pranešant atitinkamą informaciją pagal šią direktyvą. Taikant priemones, susijusias su incidentų prevencija, atskleidimu, nustatymu, apribojimu, analize ir reagavimu į juos, informuotumo apie konkrečias kibernetines grėsmes didinimo priemones, keitimąsi informacija ištaisant pažeidžiamumus ir koordinuotai juos atskleidžiant, taip pat savanorišką keitimąsi informacija apie tuos incidentus, kibernetines grėsmes ir pažeidžiamumus, užvaldymo rodiklius, taktiką, metodus ir procedūras, kibernetinio saugumo įspėjimus ir konfigūracijos priemones gali reikėti tvarkyti tam tikrų kategorijų asmens duomenis, pavyzdžiui, IP adresus, universaliuosius išteklių adresus (URL), domenų vardus, el. pašto adresus ir, kai jose atskleidžiami asmens duomenys, laiko žymas. Kompetentingų institucijų, bendrųjų kontaktinių punktų ir CSIRT vykdomas asmens duomenų tvarkymas galėtų būti teisinė prievolė arba būti laikomas būtinu siekiant atlikti užduotį viešojo intereso labui arba vykdant duomenų valdytojui pagal Reglamento (ES) 2016/679 6 straipsnio 1 dalies c arba e punktą ir 6 straipsnio 3 dalį pavestas viešosios valdžios funkcijas, arba siekiant teisėtų esminių ir svarbių subjektų interesų, kaip nurodyta to Reglamento 6 straipsnio 1 dalies f punkte. Be to, nacionalinėje teisėje galėtų būti nustatytos taisyklės, pagal kurias kompetentingoms institucijoms, bendriesiems kontaktiniams punktams ir CSIRT būtų leidžiama tiek, kiek tai būtina ir proporcinga siekiant užtikrinti esminių ir svarbių subjektų tinklų ir informacinių sistemų saugumą, tvarkyti specialių kategorijų asmens duomenis pagal Reglamento (ES) 2016/679 9 straipsnį, visų pirma numatant tinkamas ir konkrečias fizinių asmenų pagrindinių teisių ir interesų apsaugos priemones, įskaitant tokių duomenų pakartotinio naudojimo techninius apribojimus ir pažangiausių saugumo bei privatumo apsaugos priemonių, pavyzdžiui, pseudonimų suteikimo arba šifravimo, kai nuasmeninimas gali daryti didelį poveikį siekiamam tikslui, naudojimą;

(122) siekiant sustiprinti priežiūros įgaliojimus ir priemones, padedančius užtikrinti veiksmingą reikalavimų laikymąsi, šioje direktyvoje turėtų būti nustatytas būtiniausias priežiūros priemonių ir būdų, kuriais kompetentingos institucijos galėtų atlikti esminių ir svarbių subjektų priežiūrą, sąrašas. Be to, šioje direktyvoje turėtų būti nustatyta skirtinga esminių ir svarbių subjektų priežiūros tvarka, siekiant užtikrinti teisingą tiek subjektų, tiek kompetentingų institucijų pareigų pusiausvyrą. Todėl esminiams subjektams turėtų būti taikoma išsami *ex ante* ir *ex post* priežiūros tvarka, o svarbiems subjektams turėtų būti taikoma negriežta, tik *ex post*, priežiūros tvarka. Todėl iš svarbių subjektų neturėtų būti reikalaujama sistemingai dokumentuoti atitikties kibernetinio saugumo rizikos valdymo priemonėms, o kompetentingos institucijos turėtų įgyvendinti reaktyvųjį *ex post* požiūrį į priežiūrą, todėl neturėtų turėti bendros pareigos prižiūrėti tuos subjektus. Svarbių subjektų *ex post* priežiūra gali būti pradėta remiantis kompetentingoms institucijoms pateiktais įrodymais, duomenimis ar informacija, kurie, tų institucijų manymu, rodo galimus šios direktyvos pažeidimus. Pavyzdžiui, tai galėtų būti tokios pačios rūšies įrodymai, duomenys ar informacija, kuriuos kompetentingoms institucijoms pateikia kitos institucijos, subjektai, piliečiai, žiniasklaida ar kiti šaltiniai, viešai prieinama informacija arba informacija, kurią kompetentingos institucijos galėtų gauti vykdydamos kitą jų užduotims atlikti reikalingą veiklą;

(123) kompetentingoms institucijoms vykdant priežiūros užduotis neturėtų būti be reikalo trukdoma atitinkamo subjekto verslo veiklai. Kai kompetentingos institucijos vykdo savo su esminiais subjektais susijusias priežiūros užduotis, įskaitant patikrinimus vietoje ir priežiūrą ne vietoje, šios direktyvos pažeidimų tyrimą, saugumo auditus ar saugumo patikrinimus, jos turėtų kuo labiau sumažinti poveikį atitinkamo subjekto verslo veiklai;

(124) vykdydamos *ex ante* priežiūrą, kompetentingos institucijos turėtų galėti nuspręsti nustatyti prioritetus dėl proporcingo jų turimų priežiūros priemonių ir būdų naudojimo. Tai reiškia, kad kompetentingos institucijos gali nuspręsti dėl tokių prioritetų nustatymo remdamosi priežiūros metodikomis, pagal kurias turėtų būti laikomasi rizika grindžiamo požiūrio. Konkrečiau, tokios metodikos galėtų apimti esminių subjektų klasifikavimo pagal rizikos kategorijas kriterijus ar lyginamuosius standartus ir atitinkamas priežiūros priemones bei būdus, rekomenduojamus kiekvienai rizikos kategorijai, pavyzdžiui, patikrinimų vietoje, tikslinių saugumo auditų ar saugumo patikrinimų naudojimą, dažnumą ar rūšį, prašomos pateikti informacijos rūšį ir tos informacijos išsamumo lygį. Kartu su tokiomis priežiūros metodikomis taip pat galėtų būti parengiamos darbo programos ir jos

galėtų būti reguliariai vertinamos bei peržiūrimos, be kita ko, atsižvelgiant į tokius aspektus kaip išteklių paskirstymas ir poreikiai. Viešojo administravimo subjektų atžvilgiu priežiūros įgaliojimais turėtų būti naudojamasi laikantis nacionalinių teisėkūros ir institucinių sistemų;

(125) kompetentingos institucijos turėtų užtikrinti, kad su esminiais ir svarbiais subjektais susijusias jų priežiūros užduotis vykdytų kvalifikuoti specialistai, kurie turėtų turėti toms užduotims atlikti reikiamų įgūdžių, visų pirma susijusių su patikrinimų vietoje ir priežiūros ne vietoje vykdymu, įskaitant duomenų bazių, aparatinės įrangos, užkardų, šifravimo ir tinklų trūkumų nustatymą. Tie patikrinimai ir priežiūra turėtų būti vykdomi objektyviai;

(126) tinkamai pagrįstais atvejais, kai kompetentinga institucija žino apie didelę kibernetinę grėsmę arba iškilusią riziką, ji turėtų turėti galimybę nedelsiant priimti vykdymo užtikrinimo sprendimus, kad užkirstų kelią incidentui arba į jį reaguotų;

(127) kad vykdymo užtikrinimas būtų veiksmingas, turėtų būti nustatytas būtinas vykdymo užtikrinimo galių, kurias galima įgyvendinti už šioje direktyvoje nustatytų kibernetinio saugumo rizikos valdymo priemonių ir pareigų pranešti pažeidimą, sąrašas, kuriuo būtų sukurta aiški ir nuosekli tokio vykdymo užtikrinimo visoje Sąjungoje sistema. Turėtų būti deramai atsižvelgta į šios direktyvos pažeidimo pobūdį, rimtumą ir trukmę, padarytą turtinę ar neturtinę žalą, į tai, ar pažeidimas buvo padarytas tyčia ar dėl neatsargumo, veiksmus, kurių imtasi siekiant užkirsti kelią turtinei ar neturtinei žalai arba ją sumažinti, atsakomybės laipsnį ar bet kokius atitinkamus ankstesnius pažeidimus, bendradarbiavimo su kompetentinga institucija laipsnį ir visas kitas atsakomybę sunkinančias arba švelninančias aplinkybes. Vykdymo užtikrinimo priemonės, įskaitant administracines baudas, turėtų būti proporcingos ir jas skiriant turėtų būti taikomos tinkamos procedūrinės apsaugos priemonės pagal bendruosius Sąjungos teisės principus ir Europos Sąjungos pagrindinių teisių chartiją (toliau – Chartija), įskaitant teisę į veiksmingą teisinę gynybą bei teisingą bylos nagrinėjimą, nekaltumo prezumpciją ir teisę į gynybą;

(128) pagal šią direktyvą nereikalaujama, kad valstybės narės numatytų fizinių asmenų, atsakingų už tai, kad subjektas laikytųsi šios direktyvos, baudžiamąją ar civilinę atsakomybę dėl žalos, kurią trečiosios šalys patyrė dėl šios direktyvos pažeidimo;

(129) siekiant užtikrinti veiksmingą šioje direktyvoje nustatytų pareigų vykdymą, kiekvienai kompetentingai institucijai turėtų būti suteikti įgaliojimai skirti administracines baudas arba prašyti jas skirti;

(130) jei administracinė bauda skiriama esminiam ar svarbiam subjektui, kuris yra įmonė, tais tikslais įmonė turėtų būti suprantama kaip įmonė, apibrėžta SESV 101 ir 102 straipsniuose. Jei administracinė bauda skiriama asmeniui, kuris nėra įmonė, svarstydama, koks būtų tinkamas baudos dydis, kompetentinga institucija turėtų atsižvelgti į bendrą pajamų lygį valstybėje narėje ir į to asmens ekonominę padėtį. Valstybės narės turėtų nustatyti, ar ir kokiu mastu valdžios institucijoms turėtų būti skiriamos administracinės baudos. Administracinės baudos skyrimas neturi įtakos kompetentingų institucijų kitų įgaliojimų ar kitų sankcijų, nustatytų nacionalinėse taisyklėse, kuriomis ši direktyva perkeliama į nacionalinę teisę, taikymui;

(131) valstybės narės turėtų galėti nustatyti taisykles dėl baudžiamųjų sankcijų už nacionalinių taisyklių, kuriomis ši direktyva perkeliama į nacionalinę teisę, pažeidimus. Tačiau skiriant baudžiamąsias sankcijas už tokių nacionalinių taisyklių pažeidimus ir susijusias administracines sankcijas neturėtų būti pažeistas ne *bis in idem* principas, kaip jį aiškina Europos Sąjungos Teisingumo Teismas;

(132) kai šia direktyva administracinės sankcijos nėra suderintos arba kai tai yra būtina kitais atvejais, pavyzdžiui, sunkaus šios direktyvos pažeidimo atveju, valstybės narės turėtų įgyvendinti sistemą, pagal kurią numatomos veiksmingos, proporcingos ir atgrasomos sankcijos. Tokių sankcijų pobūdis ir tai, ar jos yra baudžiamosios, ar administracinės, turėtų būti nustatyta nacionalinėje teisėje;

(133) siekiant dar labiau sustiprinti vykdymo užtikrinimo priemonių, taikomų šios direktyvos pažeidimams, veiksmingumą ir atgrasomumą, kompetentingoms institucijoms turėtų būti suteikti įgaliojimai laikinai sustabdyti arba reikalauti laikinai sustabdyti sertifikavimą ar leidimą, susijusį su dalimi ar visomis atitinkamomis esminio subjekto teikiamomis paslaugomis arba vykdoma veikla, ir reikalauti nustatyti laikiną draudimą bet kuriam generalinio direktoriaus arba teisinio atstovo lygmens vadovaujamas pareigas einančiam fiziniam asmeniui eiti vadovaujamas pareigas. Atsižvelgiant į tokių laikinų sustabdymų ar draudimų griežtumą ir poveikį subjektų veiklai ir galiausiai vartotojams, jie turėtų būti taikomi tik proporcingai atsižvelgiant į pažeidimo sunkumą ir į kiekvieno konkretaus atvejo aplinkybes, įskaitant tai, ar pažeidimas padarytas tyčia ar dėl neatsargumo, ir veiksmus, kurių galimai imtasi siekiant užkirsti kelią turtinei ar neturtinei žalai arba ją sumažinti. Tokie laikini sustabdymai ar draudimai turėtų būti taikomi tik kaip kraštutinė priemonė, t. y. tik po to, kai išnaudojamos kitos šioje direktyvoje nustatytos atitinkamos vykdymo užtikrinimo priemonės, ir tik tol, kol atitinkamas subjektas imasi reikiamų veiksmų trūkumams ištaisyti arba kompetentingos institucijos reikalavimams, dėl kurių taikomi tokie laikini sustabdymai ar draudimai, įvykdyti. Skiriant tokius laikinus sustabdymus ar draudimus, turėtų būti taikomos tinkamos procedūrinės apsaugos priemonės pagal bendruosius Sąjungos teisės ir Chartijos principus, įskaitant teisę į veiksmingą teisinę gynybą bei teisingą bylos nagrinėjimą, nekaltumo prezumpciją ir teisę į gynybą;

(134) siekdamos užtikrinti, kad subjektai laikytųsi savo pareigų, nustatytų šioje direktyvoje, valstybės narės turėtų bendradarbiauti ir padėti viena kitai priežiūros ir vykdymo užtikrinimo priemonių srityje, visų pirma tais atvejais, kai subjektas teikia paslaugas daugiau nei vienoje valstybėje narėje arba kai jo tinklų ir informacinės sistemos yra kitoje valstybėje narėje nei ta, kurioje jis teikia paslaugas. Prašymą gavusi kompetentinga institucija, teikdama pagalbą, turėtų imtis priežiūros arba vykdymo užtikrinimo priemonių laikydamasi nacionalinės teisės. Siekdamos užtikrinti sklandų savitarpio pagalbos pagal šią direktyvą veikimą, kompetentingos institucijos turėtų naudotis Bendradarbiavimo grupe kaip forumu atvejams ir konkretiems pagalbos prašymams aptarti;

(135) siekiant užtikrinti veiksmingą priežiūrą ir vykdymo užtikrinimą, visų pirma, kai situacija yra tarpvalstybinio pobūdžio, valstybė narė, gavusi savitarpio pagalbos prašymą, turėtų, neviršydama to prašymo ribų, imtis tinkamų priežiūros ir vykdymo užtikrinimo priemonių subjekto, kuris yra to prašymo objektas ir kuris teikia paslaugas arba turi tinklų ir informacinę sistemą tos valstybės narės teritorijoje;

(136) šia direktyva turėtų būti nustatytos kompetentingų institucijų ir priežiūros institucijų pagal Reglamentą (ES) 2016/679 bendradarbiavimo taisyklės, siekiant nagrinėti šios direktyvos pažeidimus, susijusius su asmens duomenimis;

(137) šia direktyva turėtų būti siekiama užtikrinti aukšto lygio esminių ir svarbių subjektų atsakomybę už kibernetinio saugumo rizikos valdymo priemones ir pareigas pranešti. Todėl esminių ir svarbių subjektų valdymo organai turėtų patvirtinti kibernetinio saugumo rizikos valdymo priemones ir prižiūrėti jų įgyvendinimą;

(138) siekiant užtikrinti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje šios direktyvos pagrindu, pagal SESV 290 straipsnį Komisijai turėtų būti deleguoti įgaliojimai priimti aktus dėl šios direktyvos papildymo, nurodant, iš kokių kategorijų esminių ir svarbių subjektų reikalaujama naudoti tam tikrus sertifikuotus IRT produktus, IRT paslaugas ir IRT procesus arba gauti sertifikatą pagal Europos kibernetinio saugumo sertifikavimo schemą. Ypač svarbu, kad atlikdama parengiamąjį darbą Komisija tinkamai konsultuotųsi, taip pat ir su ekspertais, ir kad tos konsultacijos būtų vykdomos vadovaujantis 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros ([22]) nustatytais principais. Visų pirma siekiant užtikrinti vienodas galimybes dalyvauti atliekant su deleguotaisiais aktais susijusį parengiamąjį darbą, Europos Parlamentas ir Taryba visus dokumentus gauna tuo pačiu metu kaip ir valstybių narių ekspertai, o jų ekspertams sistemingai suteikiama galimybė dalyvauti Komisijos ekspertų grupių, kurios atlieka su deleguotaisiais aktais susijusį parengiamąjį darbą, posėdžiuose;

([22]) OL L 123, 2016 5 12, p. 1.

(139) siekiant užtikrinti vienodas šios direktyvos įgyvendinimo sąlygas, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai nustatyti Bendradarbiavimo grupės veikimui būtiną procedūrinę tvarką ir techninius bei metodinius, taip pat sektorinius reikalavimus, susijusius su kibernetinio saugumo rizikos valdymo priemonėmis, ir išsamiau apibrėžti pranešimų apie incidentus, kibernetinę grėsmę ir vos neįvykusius incidentus bei informuojant apie didelę kibernetinę grėsmę pateikiamos informacijos rūšį, formą ir tvarką, taip pat atvejus, kuriais incidentas turi būti laikomas dideliu. Tais įgaliojimais turėtų būti naudojamasi laikantis Europos Parlamento ir Tarybos reglamento (ES) Nr. 182/2011 ([23]);

(140) Komisija, pasikonsultavusi su suinteresuotaisiais subjektais, turėtų periodiškai peržiūrėti šią direktyvą, visų pirma siekdama nustatyti, ar tikslinga siūlyti pakeitimus atsižvelgiant į kintančias visuomenines, politines, technologines ar rinkos sąlygas. Atlikdama tas peržiūras, Komisija turėtų įvertinti susijusių subjektų dydžio ir šios direktyvos prieduose nurodytų sektorių, subsektorių ir subjektų rūšių svarbą ekonomikos ir visuomenės veikimui kibernetinio saugumo atžvilgiu. Komisija turėtų, *inter alia*, įvertinti, ar paslaugų teikėjai, kuriems taikoma ši direktyva, pripažinti kaip labai didelės interneto platformos, kaip tai suprantama Europos Parlamento ir Tarybos reglamento (ES) 2022/2065 ([24]) 33 straipsnyje, gali būti identifikuoti kaip esminiai subjektai pagal šią direktyvą;

(141) šia direktyva sukuriamos naujos ENISA užduotys, taip sustiprinant jos vaidmenį, ir dėl to ENISA gali būti keliami reikalavimai vykdyti savo esamas užduotis pagal Reglamentą (ES) 2019/881 aukštesniu lygiu nei anksčiau. Siekiant užtikrinti, kad ENISA turėtų finansinių ir žmogiškųjų išteklių, kurių reikia, kad ji vykdytų esamas ir naujas užduotis, taip pat atitiktų bet kokį aukštesnį tų užduočių vykdymo lygį, susijusį su jos sustiprintu vaidmeniu, jos biudžetas turėtų būti atitinkamai padidintas. Be to, siekiant užtikrinti veiksmingą išteklių panaudojimą, ENISA turėtų būti suteikta daugiau lankstumo, sudarant jai sąlygas skirstyti išteklius viduje siekiant, kad ji veiksmingai vykdytų savo užduotis ir patenkintų lūkesčius;

(142) kadangi šios direktyvos tikslo, t. y. užtikrinti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje, valstybės narės negali deramai pasiekti, o dėl siūlomo veiksmo poveikio to tikslo būtų geriau siekti Sąjungos lygmeniu, 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;

(143) šia direktyva paisoma pagrindinių teisių ir laikomasi principų, pripažįstamų Chartijoje, visų pirma teisės į tai, kad būtų gerbiamas privatus gyvenimas bei komunikacijos slaptumas, teisės į asmens duomenų apsaugą, laisvės užsiimti verslu, teisės į nuosavybę, teisės į veiksmingą teisinę gynybą ir teisingą bylos nagrinėjimą, nekaltumo prezumpcijos ir teisės į gynybą. Teisė į veiksmingą teisinę gynybą užtikrinama ir esminių ir svarbių subjektų teikiamų paslaugų gavėjams. Ši direktyva turėtų būti įgyvendinta atsižvelgiant į tas teises ir principus;

(144) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([25]) 42 straipsnio 1 dalimi buvo pasikonsultuota su Europos duomenų apsaugos priežiūros pareigūnu, ir 2021 m. kovo 11 d. jis pateikė savo nuomonę ([26]),

([23]) 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).

([24]) 2022 m. spalio 19 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2065 dėl skaitmeninių paslaugų bendrosios rinkos, kuriuo iš dalies keičiama Direktyva 2000/31/EB (Skaitmeninių paslaugų aktas) (OL L 277, 2022 10 27, p. 1).

([25]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39).

([26]) OL C 183, 2021 5 11, p. 3.

PRIĖMĖ ŠIĄ DIREKTYVĄ:

I SKYRIUS

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas

1. Šia direktyva nustatomos priemonės, kuriomis siekiama užtikrinti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje, kad būtų pagerintas vidaus rinkos veikimas.

2. Tuo tikslu šia direktyva nustatomos:

a) pareigos, kuriomis iš valstybių narių reikalaujama priimti nacionalines kibernetinio saugumo strategijas ir paskirti arba įsteigti kompetentingas institucijas, kibernetinių krizių valdymo institucijas, bendruosius kibernetinio saugumo kontaktinius punktus (toliau – bendrieji kontaktiniai punktai) ir reagavimo į kompiuterių saugumo incidentus tarnybas (CSIRT);

b) kibernetinio saugumo rizikos valdymo priemonės ir pareigos pranešti, taikomos I ar II priede nurodytos rūšies subjektams, taip pat subjektams, identifikuotiems kaip ypatingos svarbos subjektai pagal Direktyvą (ES) 2022/2557;

c) dalijimosi kibernetinio saugumo informacija taisyklės ir pareigos ja dalytis;

d) valstybių narių pareigos priežiūros ir vykdymo užtikrinimo srityse.

2 straipsnis

Taikymo sritis

1. Ši direktyva taikoma I ar II priede nurodytos rūšies viešiesiems ar privatiesiems subjektams, kurie laikomi vidutinėmis įmonėmis pagal Rekomendacijos 2003/361/EB priedo 2 straipsnį arba kurie viršija to straipsnio 1 dalyje nustatytas viršutines ribas, ir kurie teikia paslaugas arba vykdo veiklą Sąjungoje.

Šios direktyvos tikslais tos rekomendacijos priedo 3 straipsnio 4 dalis netaikoma.

2. Nepaisant subjektų dydžio, ši direktyva taip pat taikoma I ar II priede nurodytos rūšies subjektams, kai:

a) paslaugas teikia:

   i) viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai;

   ii) patikimumo užtikrinimo paslaugų teikėjai;

   iii) aukščiausio lygio domenų vardų registrai ir domenų vardų sistemos paslaugų teikėjai;

b) subjektas yra vienintelis paslaugos, kuri yra būtina siekiant užtikrinti ypatingos svarbos visuomeninės ar ekonominės veiklos vykdymą, teikėjas valstybėje narėje;

c) paslaugos, kurią teikia subjektas, sutrikimas galėtų daryti didelį poveikį viešajam saugumui, visuomenės saugumui arba visuomenės sveikatai;

d) paslaugos, kurią teikia subjektas, sutrikimas galėtų kelti didelę sisteminę riziką visų pirma sektoriuose, kuriuose toks sutrikimas galėtų daryti tarpvalstybinį poveikį;

e) subjektas yra ypatingos svarbos atsižvelgiant į jo konkrečią svarbą konkrečiam sektoriui ar paslaugos rūšiai arba kitiems tarpusavyje priklausomiems sektoriams valstybėje narėje nacionaliniu ar regioniniu lygmeniu;

f) subjektas yra:

i) centrinės valdžios, kaip valstybė narė apibrėžė pagal nacionalinę teisę viešojo administravimo subjektas, arba

ii) regioninio lygmens, kaip valstybė narė apibrėžė pagal nacionalinę teisę, kuris, atlikus rizika grindžiamą vertinimą, teikia paslaugas, kurių sutrikimas galėtų daryti didelį poveikį ypatingos svarbos visuomeninei ar ekonominei veiklai, viešojo administravimo subjektas.

3. Nepriklausomai nuo jų dydžio, ši direktyva taikoma subjektams, identifikuotiems kaip ypatingos svarbos subjektai pagal Direktyvą (ES) 2022/2557.

4. Nepriklausomai nuo jų dydžio, ši direktyva taikoma subjektams, teikiantiems domenų vardų registravimo paslaugas.

5. Valstybės narės gali numatyti, kad ši direktyva taikoma:

a) viešojo administravimo subjektams vietos lygmeniu;

b) švietimo įstaigoms, visų pirma tais atvejais, kai jos vykdo ypatingos svarbos mokslinių tyrimų veiklą.

6. Šia direktyva nedaromas poveikis valstybių narių atsakomybei užtikrinti nacionalinį saugumą ir jų įgaliojimams apsaugoti kitas esmines valstybines funkcijas, įskaitant valstybės teritorinio vientisumo užtikrinimą ir viešosios tvarkos palaikymą.

7. Ši direktyva netaikoma viešojo administravimo subjektams, vykdantiems savo veiklą, nacionalinio saugumo, visuomenės saugumo, gynybos ar teisėsaugos srityse, įskaitant nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas.

8. Valstybės narės gali atleisti nuo 21 ir 23 straipsniuose nustatytų pareigų konkrečius subjektus, vykdančius veiklą nacionalinio saugumo, visuomenės saugumo, gynybos ar teisėsaugos srityse, įskaitant nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas, arba kurie teikia paslaugas išimtinai šio straipsnio 7 dalyje nurodytiems viešojo administravimo subjektams, tos veiklos ar paslaugų atžvilgiu. Tokiais atvejais VII skyriuje nurodytos priežiūros ir vykdymo užtikrinimo priemonės netaikomos tai konkrečiai veiklai ar paslaugoms. Kai subjektai vykdo tik šioje dalyje nurodytos rūšies veiklą arba teikia tik šioje dalyje nurodytos rūšies paslaugas, valstybės narės taip pat gali nuspręsti atleisti tuos subjektus nuo 3 ir 27 straipsniuose nustatytų pareigų.

9. 7 ir 8 dalys netaikomos, kai subjektas veikia kaip patikimumo užtikrinimo paslaugų teikėjas.

10. Ši direktyva netaikoma subjektams, kuriems valstybės narės netaiko Reglamento (ES) 2022/2554 pagal to reglamento 2 straipsnio 4 dalį.

11. Šioje direktyvoje nustatytos pareigos nereiškia, kad bus teikiama informacija, kurios atskleidimas prieštarautų esminiams valstybių narių nacionalinio saugumo, viešojo saugumo ar gynybos interesams.

12. Ši direktyva taikoma nedarant poveikio Reglamentui (ES) 2016/679, Direktyvai 2002/58/EB, Europos Parlamento ir Tarybos direktyvoms 2011/93/ES ([27]) ir 2013/40/ES ([28]) ir Direktyvai (ES) 2022/2557.

13. Nedarant poveikio SESV 346 straipsniui, informacija, kuri yra konfidenciali pagal Sąjungos ar nacionalines taisykles, kaip antai taisyklės dėl verslo konfidencialumo, turi būti pagal šią direktyvą keičiamasi su Komisija ir kitomis atitinkamomis institucijomis tik tais atvejais, kai toks keitimasis yra būtinas šios direktyvos taikymui. Keičiamasi tik tokia informacija, kuri atitinka keitimosi tikslą ir yra jam proporcinga. Keičiantis informacija saugomas tos informacijos konfidencialumas ir atitinkamų subjektų saugumo ir komerciniai interesai.

([27]) 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).

([28]) 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).

14. Subjektai, kompetentingos institucijos, bendrieji kontaktiniai punktai ir CSIRT tvarko asmens duomenis tiek, kiek tai būtina šios direktyvos tikslais ir laikydamiesi Reglamento (ES) 2016/679, ir toks tvarkymas visų pirma grindžiamas to reglamento 6 straipsniu.

Asmens duomenų tvarkymą pagal šią direktyvą viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai vykdo laikydamiesi Sąjungos duomenų apsaugos teisės ir Sąjungos privatumo teisės, visų pirma Direktyvos 2002/58/EB, nuostatų.

3 straipsnis

Esminiai ir svarbūs subjektai

1. Šios direktyvos taikymo tikslais esminiais subjektais laikomi šie subjektai:

a) I priede nurodytos rūšies subjektai, kurie viršija vidutinėms įmonėms nustatytas viršutines ribas, nustatytas Rekomendacijos 2003/361/EB priedo 2 straipsnio 1 dalyje;

b) kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai ir aukščiausio lygio domenų vardų registrai, taip pat DNS paslaugų teikėjai, nepriklausomai nuo jų dydžio;

c) viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai, kurie laikomi vidutinėmis įmonėmis pagal Rekomendacijos 2003/361/EB priedo 2 straipsnį;

d) 2 straipsnio 2 dalies f punkto i papunktyje nurodyti viešojo administravimo subjektai;

e) visi kiti I arba II priede nurodytos rūšies subjektai, kuriuos valstybė narė identifikavo kaip esminius subjektus pagal 2 straipsnio 2 dalies b-e punktus;

f) subjektai, kurie pagal Direktyvą (ES) 2022/2557 identifikuoti kaip ypatingos svarbos subjektai, nurodyti šios direktyvos 2 straipsnio 3 dalyje;

g) jei valstybė narė taip numato, subjektai, kuriuos ta valstybė narė ne vėliau kaip 2023 m. sausio 16 d. identifikavo kaip esminių paslaugų operatorius pagal Direktyvą (ES) 2016/1148 arba nacionalinę teisę.

2. Šios direktyvos I arba II priede nurodytos rūšies subjektai, kurie nelaikomi esminiais subjektais pagal šio straipsnio 1 dalį, laikomi svarbiais subjektais. Tai apima subjektus, kuriuos valstybė narė identifikavo kaip esminius subjektus pagal 2 straipsnio 2 daliesb–e punktus.

3. Ne vėliau kaip 2025 m. balandžio 17 d. valstybės narės sudaro esminių ir svarbių subjektų bei domeno vardo registravimo paslaugas teikiančių subjektų sąrašą. Po tos datos valstybės narės reguliariai ir ne rečiau kaip kas dvejus metus peržiūri tą sąrašą ir, kai tinkama, jį atnaujina.

4. Siekdamos sudaryti 3 dalyje nurodytą sąrašą, valstybės narės reikalauja, kad toje dalyje nurodyti subjektai kompetentingoms institucijoms pateiktų bent šią informaciją:

a) subjekto pavadinimą;

b) adresą ir naujausius kontaktinius duomenis, įskaitant subjektų el. pašto adresus, IP adresų ruožus ir telefonų numerius;

c) kai taikytina, I arba II priede nurodytą atitinkamą sektorių ir subsektorių ir

d) kai taikytina, valstybių narių, kuriose jos teikia į šios direktyvos taikymo sritį patenkančias paslaugas, sąrašą.

3 dalyje nurodyti subjektai nedelsdami ir bet kuriuo atveju ne vėliau kaip per dvi savaites nuo pakeitimo dienos praneša apie bet kokius pagal šios dalies pirmą pastraipą pateiktų duomenų pakeitimus.

Komisija, padedant Europos Sąjungos kibernetinio saugumo agentūrai (toliau – ENISA), nepagrįstai nedelsdama pateikia gaires ir šablonus, susijusius su šioje dalyje nustatytomis pareigomis.

Valstybės narės gali nustatyti nacionalinius mechanizmus, pagal kuriuos subjektai galėtų užsiregistruoti patys.

5. Ne vėliau kaip 2025 m. balandžio 17 d., o vėliau – kas dvejus metus kompetentingos institucijos praneša:

a) Komisijai ir Bendradarbiavimo grupei esminių ir svarbių subjektų, įtrauktų į sąrašą vadovaujantis 3 dalimi pagal kiekvieną iš I arba II priede nurodytų sektorių ir subsektorių, skaičių, ir

b) Komisijai – atitinkamą informaciją apie esminių ir svarbių subjektų, identifikuotų pagal 2 straipsnio 2 dalies b–e punktus, skaičių, I arba II priede nurodytą sektorių ir subsektorių, kuriems jie priklauso, jų teikiamų paslaugų rūšį ir nuostatą iš įtvirtintųjų 2 straipsnio 2 dalies b–e punktuose, pagal kurią jie buvo identifikuoti.

6. Iki 2025 m. balandžio 17 d. ir Komisijai paprašius, valstybės narės gali pranešti Komisijai 5 dalies b punkte nurodytų esminių ir svarbių subjektų pavadinimus.

4 straipsnis

Konkretiems sektoriams taikomi Sąjungos teisės aktai

1. Jei pagal konkretiems sektoriams taikomus Sąjungos teisės aktus reikalaujama, kad esminiai arba svarbūs subjektai priimtų kibernetinio saugumo rizikos valdymo priemones arba praneštų apie didelius incidentus, ir jei tų reikalavimų poveikis yra bent lygiavertis šioje direktyvoje nustatytų pareigų poveikiui, atitinkamos šios direktyvos nuostatos, įskaitant VII skyriuje įtvirtintas nuostatas dėl priežiūros ir vykdymo užtikrinimo, tokiems subjektams netaikomos. Jei konkretiems sektoriams taikomi Sąjungos teisės aktai taikomi ne visiems konkretaus sektoriaus, kuriam taikoma ši direktyva, subjektams, atitinkamos šios direktyvos nuostatos toliau taikomos subjektams, kuriems netaikomi tie konkretiems sektoriams taikomi Sąjungos teisės aktai.

2. Šio straipsnio 1 dalyje nurodytų reikalavimų poveikis laikomas lygiaverčiu šioje direktyvoje nustatytų pareigų poveikiui, jeigu:

a) kibernetinio saugumo rizikos valdymo priemonių poveikis yra bent lygiavertis priemonių, nustatytų 21 straipsnio 1 ir 2 dalyse, poveikiui; arba

b) konkrečiam sektoriui taikomame Sąjungos teisės akte numatyta CSIRT, kompetentingų institucijų arba bendrųjų kontaktinių punktų pagal šią direktyvą neatidėliotina prieiga, kai tinkama, automatinė ir tiesioginė, prie pateiktų pranešimų apie incidentus ir jei reikalavimai pranešti apie didelius incidentus yra pagal poveikį bent lygiaverčiai šios direktyvos 23 straipsnio 1–6 dalyse nustatytiems reikalavimams.

3. Komisija ne vėliau kaip 2023 m. liepos 17 d. pateikia gaires, kuriomis paaiškinamas 1 ir 2 dalių taikymas. Komisija reguliariai peržiūri tas gaires. Rengdama tas gaires Komisija atsižvelgia į visas Bendradarbiavimo grupės ir ENISA pastabas.

5 straipsnis

Minimalus suderinimas

Šia direktyva valstybėms narėms netrukdoma priimti arba palikti toliau galioti nuostatų, kuriomis užtikrinamas aukštesnio lygio kibernetinis saugumas, su sąlyga, kad tokios nuostatos yra suderinamos su valstybių narių įsipareigojimais, nustatytais Sąjungos teisėje.

6 straipsnis

Terminų apibrėžtys

Šioje direktyvoje vartojamų terminų apibrėžtys:

1) tinklų ir informacinė sistema – tai:

   a) elektroninių ryšių tinklas, kaip apibrėžta Direktyvos (ES) 2018/1972 2 straipsnio 1 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 atspariems bet kokiam įvykiui, galinčiam sukelti pavojų saugomų, perduodamų ar tvarkomų duomenų, arba teikiamų ar per tas tinklų ir informacines sistemas gaunamų paslaugų prieinamumui, autentiškumui, vientisumui ar konfidencialumui;

3) kibernetinis saugumas – kibernetinis saugumas, kaip apibrėžta Reglamento (ES) 2019/881 2 straipsnio 1 punkte;

4) nacionalinė kibernetinio saugumo strategija – nuosekli valstybės narės sistema, kurioje nustatyti tos valstybės narės kibernetinio saugumo srities strateginiai tikslai ir prioritetai ir jų įgyvendinimo valdymas;

5) vos neįvykęs incidentas – įvykis, kuriuo galėjo būti sukeltas pavojus saugomų, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumui, autentiškumui, vientisumui arba konfidencialumui, bet kuriam įvykti buvo sėkmingai užkirstas kelias arba kuris neįvyko;

6) incidentas – įvykis, kuriuo sukeliamas pavojus saugomų, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumui, autentiškumui, vientisumui arba konfidencialumui;

7) didelio masto kibernetinio saugumo incidentas – incidentas, į kurio sukeltą sutrikimą viena valstybė narė nepajėgia reaguoti arba kuris daro didelį poveikį ne mažiau kaip dviem valstybėms narėms;

8) incidento valdymas – visi veiksmai ir procedūros, kuriais siekiama užkirsti incidentui kelią, atskleisti, išanalizuoti ir sustabdyti incidentą arba į jį reaguoti ir atstatyti veiklą po incidento;

9) rizika – potencialus praradimas arba sutrikimas, kurį sukėlė incidentas, kuri turi būti išreikšta kaip tokio praradimo arba sutrikimo masto ir incidento pasikartojimo derinys;

10) kibernetinė grėsmė – kibernetinė grėsmė, kaip apibrėžta Reglamento (ES) 2019/881 2 straipsnio 8 punkte;

11) didelė kibernetinė grėsmė – kibernetinė grėsmė, dėl kurios techninių charakteristikų galima daryti prielaidą, kad ji gali padaryti didelį neigiamą poveikį subjekto tinklų ir informacinėms sistemoms arba subjekto paslaugų naudotojų tinklų ir informacinėms sistemoms, sukeldama didelę turtinę arba neturtinę žalą;

12) IRT produktas – IRT produktas, kaip apibrėžta Reglamento (ES) 2019/881 2 straipsnio 12 punkte;

13) IRT paslauga – IRT paslauga, kaip apibrėžta Reglamento (ES) 2019/881 2 straipsnio 13 punkte;

14) IRT procesas – IRT procesas, kaip apibrėžta Reglamento (ES) 2019/881 2 straipsnio 14 punkte;

15) pažeidžiamumas – IRT produktų arba IRT paslaugų silpnoji vieta, jautrumas ar trūkumas, kuriais gali būti pasinaudota kibernetinei grėsmei kelti;

16) standartas – standartas, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) Nr. 1025/2012 ([29]) 2 straipsnio 1 punkte;

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

([29]) 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).

18) interneto duomenų srautų mainų taškas – tinklo įrenginys, kuris sudaro sąlygas sujungti daugiau nei du nepriklausomus tinklus (autonomines sistemas), visų pirma siekiant palengvinti interneto duomenų srautų mainus, kuris sujungia tik autonomines sistemas ir kuris nereikalauja, kad interneto duomenų srautai, perduodami tarp bet kurių naudojamų autonominių sistemų porų, būtų perduodami per bet kurią trečią autonominę sistemą ir nekeičia tokių srautų ar kitokiu būdu jų netrikdo;

19) domenų vardų sistema arba DNS – hierarchiškai paskirstyta vardų sistema, kurioje galima identifikuoti interneto paslaugas ir išteklius ir sudaromos sąlygos galutiniams naudotojams naudotis interneto maršruto parinkimo ir junglumo paslaugomis ir gauti tas paslaugas bei išteklius;

20) DNS paslaugų teikėjas – subjektas, kuris teikia:

a) viešai prieinamas rekursinio domenų vardų keitimo paslaugas galutiniams interneto naudotojams arba

b) patikimo domenų vardų keitimo paslaugas trečiųjų šalių reikmėms, išskyrus šakninio pavadinimo serverius;

21) aukščiausio lygio domenų vardų registras – subjektas, kuriam pavestas konkretus aukščiausio lygio domenas ir kuris atsako už aukščiausio lygio domeno administravimą, įskaitant to aukščiausio lygio domeno domenų vardų registraciją ir techninį to aukščiausio lygio domeno veikimą, įskaitant jo vardų serverių veikimą, duomenų bazių techninę priežiūrą ir aukščiausio lygio domenų zonos rinkmenų paskirstymą tarp vardų serverių, neatsižvelgiant į tai, ar bet kurias iš tų operacijų atlieka pats subjektas, ar tai yra užsakomosios paslaugos, tačiau neįtraukiant atvejų, kai registras aukščiausio lygio domenų vardus naudoja tik savo reikmėms;

22) domenų vardų registravimo paslaugas teikiantis subjektas – registratorius arba registratorių vardu veikiantis agentas, pavyzdžiui, privatumo ar įgaliotojo serverio registravimo paslaugų teikėjas arba perpardavėjas;

23) skaitmeninė paslauga – paslauga, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2015/1535 ([30]) 1 straipsnio 1 dalies b punkte;

24) patikimumo užtikrinimo paslauga – patikimumo užtikrinimo paslauga, kaip apibrėžta Reglamento (ES) Nr. 910/2014 3 straipsnio 16 punkte;

25) patikimumo užtikrinimo paslaugų teikėjas – patikimumo užtikrinimo paslaugų teikėjas, kaip apibrėžta Reglamento (ES) Nr. 910/2014 3 straipsnio 19 punkte;

26) kvalifikuota patikimumo užtikrinimo paslauga – kvalifikuota patikimumo užtikrinimo paslauga, kaip apibrėžta Reglamento (ES) Nr. 910/2014 3 straipsnio 17 punkte;

27) kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas – kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, kaip apibrėžta Reglamento (ES) Nr. 910/2014 3 straipsnio 20 punkte;

28) elektroninė prekyvietė – elektroninė prekyvietė, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2005/29/EB ([31]) 2 straipsnio n punkte;

29) interneto paieškos sistema – interneto paieškos sistema, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2019/1150 ([32]) 2 straipsnio 5 punkte;

30) debesijos kompiuterijos paslauga – skaitmeninė paslauga, kuri pagal poreikį suteikia administravimo paslaugas ir plataus masto nuotolinę prieigą prie kintamo masto pritaikomos bendrų ir paskirstytų kompiuterijos išteklių bazės, įskaitant atvejus, kai tokie ištekliai yra paskirstyti per kelias vietas;

([30]) 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).

([31]) 2005 m. gegužės 11 d. Europos Parlamento ir Tarybos direktyva 2005/29/EB dėl nesąžiningos įmonių komercinės veiklos vartotojų atžvilgiu vidaus rinkoje ir iš dalies keičianti Tarybos direktyvą 84/450/EEB, Europos Parlamento ir Tarybos direktyvas 97/7/EB, 98/27/EB bei 2002/65/EB ir Europos Parlamento ir Tarybos reglamentą (EB) Nr. 2006/2004 („Nesąžiningos komercinės veiklos direktyva“) (OL L 149, 2005 6 11, p. 22).

([32]) 2019 m. birželio 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/1150 dėl verslo klientams teikiamų internetinių tarpininkavimo paslaugų sąžiningumo ir skaidrumo didinimo (OL L 186, 2019 7 11, p. 57).

31) duomenų centro paslauga – paslauga, kuri apima struktūras arba struktūrų grupes, skirtas IT ir tinklo įrangos centralizuotam pritaikymui, tarpusavio junglumui ir eksploatavimui, teikiant duomenų saugojimo, tvarkymo ir transportavimo paslaugas kartu su visa energijos paskirstymo ir aplinkos kontrolės įranga ir infrastruktūra;

32) turinio teikimo tinklas – geografiškai paskirstytų serverių tinklas, kurio paskirtis yra turinio ir paslaugų teikėjų vardu užtikrinti interneto naudotojams didelę skaitmeninio turinio ir paslaugų pasiūlą, prieinamumą arba greitą teikimą;

33) socialinių tinklų paslaugų platforma – platforma, kurioje galutiniams naudotojams sudaromos sąlygos prisijungti, dalytis, rasti vienas kitą ir bendrauti naudojant įvairius prietaisus, visų pirma per pokalbius, įrašus, vaizdo įrašus ir rekomendacijas;

34) atstovas – Sąjungoje įsisteigęs fizinis arba juridinis asmuo, paskirtas veikti tik DNS paslaugų teikėjo, aukščiausio lygio domenų vardų registro, domenų vardų registravimo paslaugas teikiančio subjekto, debesijos kompiuterijos paslaugų teikėjo, duomenų centro paslaugų teikėjo, turinio pristatymo tinklo paslaugų teikėjo, valdomų paslaugų teikėjo, valdomų saugumo paslaugų teikėjo, elektroninės prekyvietės paslaugų teikėjo, interneto paieškos sistemos paslaugų teikėjo arba socialinio tinklo paslaugų platformų paslaugų teikėjo, kuris nėra įsisteigęs Sąjungoje, vardu, į kurį kompetentinga institucija arba CSIRT gali kreiptis vietoj subjekto dėl to subjekto pareigų pagal šią direktyvą;

35) viešojo administravimo subjektas – valstybės narės subjektas, kuris valstybėje narėje pagal nacionalinę teisę yra pripažįstamas tokiu subjektu, išskyrus teismines institucijas, parlamentus ir centrinius bankus, ir kuris atitinka šiuos kriterijus:

   a) yra įsteigtas siekiant tikslo tenkinti bendrojo intereso poreikius, ir nėra pramoninio ar komercinio pobūdžio;

   b) turi juridinio asmens statusą arba pagal teisės aktus turi teisę veikti kito juridinio asmens statusą turinčio subjekto vardu;

   c) didžiąja dalimi yra finansuojamas valstybės, regioninių institucijų ar kitų viešosios teisės reglamentuojamų įstaigų lėšomis, arba jam taikoma tų institucijų ar įstaigų administracinė priežiūra, arba jis turi administracinį, valdymo ar priežiūros organą, kurio daugiau kaip pusę narių skiria valstybės, regioninės institucijos arba kitos viešosios teisės reglamentuojamos įstaigos;

   d) turi įgaliojimus priimti administracinius arba reguliavimo sprendimus dėl fizinių arba juridinių asmenų, kurie daro poveikį jų teisėms tarpvalstybinio asmenų, prekių, paslaugų ar kapitalo judėjimo srityje;

36) viešasis elektroninių ryšių tinklas – viešasis elektroninių ryšių tinklas, kaip apibrėžta Direktyvos (ES) 2018/1972 2 straipsnio 8 punkte;

37) elektroninių ryšių paslauga – elektroninių ryšių paslauga, kaip apibrėžta Direktyvos (ES) 2018/1972 2 straipsnio 4 punkte;

38) subjektas – fizinis asmuo arba juridinis asmuo, įsteigtas ir tokiu pripažintas pagal jo įsteigimo vietos nacionalinę teisę, kuris, veikdamas savo vardu, naudojasi teisėmis ir kuriam gali būti taikomos pareigos;

39) valdomų paslaugų teikėjas – subjektas, teikiantis paslaugas, susijusias su IRT produktų, tinklų, infrastruktūros, taikomųjų programų ar bet kurių kitų tinklų ir informacinių sistemų diegimu, valdymu, naudojimu ar technine priežiūra, teikdamas pagalbą arba aktyvaus administravimo paslaugas klientų patalpose arba nuotoliniu būdu;

40) valdomų saugumo paslaugų teikėjas – valdomų paslaugų teikėjas, vykdantis veiklą, susijusią su kibernetinio saugumo rizikos valdymu, arba teikiantis pagalbą tokiai veiklai;

41) mokslinių tyrimų organizacija – subjektas, kurio pagrindinis tikslas – vykdyti taikomuosius mokslinius tyrimus arba eksperimentinę plėtrą, siekiant panaudoti tų mokslinių tyrimų rezultatus komerciniais tikslais, tačiau kurio veikla neapima švietimo įstaigų.

II SKYRIUS

KOORDINUOTOS KIBERNETINĖS SISTEMOS

7 straipsnis

Nacionalinė kibernetinio saugumo strategija

1. Kiekviena valstybė narė priima nacionalinę kibernetinio saugumo strategiją, kurioje nustatomi strateginiai tikslai, reikiami ištekliai tiems tikslams pasiekti ir tinkamos politikos bei reguliavimo priemonės, kad būtų pasiektas ir išlaikytas aukšto lygmens kibernetinis saugumas. Nacionalinė kibernetinio saugumo strategija apima:

a) valstybės narės kibernetinio saugumo strategijos tikslus ir prioritetus, visų pirma apimančius I ir II prieduose nurodytus sektorius;

b) valdymo sistemą, kad būtų pasiekti šios dalies a punkte nurodyti tikslai ir įgyvendinti prioritetai, įskaitant 2 dalyje nurodytą politiką;

c) valdymo sistemą, pagal kurią paaiškinami atitinkamų suinteresuotųjų subjektų vaidmenys ir pareigos nacionaliniu lygmeniu, kuria grindžiamas kompetentingų institucijų, bendrųjų kontaktinių punktų ir CSIRT pagal šią direktyvą bendradarbiavimas ir veiklos koordinavimas nacionaliniu lygmeniu, taip pat tų įstaigų ir kompetentingų institucijų pagal konkretiems sektoriams taikomus Sąjungos teisės aktus veiklos koordinavimas ir jų bendradarbiavimas;

d) mechanizmą, pagal kurį nustatomi atitinkami objektai, ir kibernetinio saugumo rizikų toje valstybėje narėje vertinimą;

e) parengties, reagavimo į incidentus ir veiklos po incidento atstatymo priemonių, įskaitant viešojo ir privačiojo sektorių bendradarbiavimą, nustatymą;

f) įvairių institucijų ir suinteresuotųjų subjektų, dalyvaujančių įgyvendinant nacionalinę kibernetinio saugumo strategiją, sąrašą;

g) politikos sistemą, padedančią užtikrinti geresnį kompetentingų institucijų pagal šią direktyvą ir kompetentingų institucijų pagal Direktyvą (ES) 2022/2557 koordinavimą siekiant dalytis informacija apie rizikas, kibernetines grėsmes, ir incidentus, taip pat apie nekibernetinę riziką, grėsmes ir incidentus bei, prireikus, vykdyti priežiūros užduotis;

h) planą, įskaitant būtinas priemones, piliečių informuotumo apie kibernetinį saugumą bendram lygiui didinti.

2. Nacionalinėje kibernetinio saugumo strategijoje valstybės narės visų pirma nustato:

a) politiką dėl IRT produktų ir IRT paslaugų, kuriuos subjektai naudoja teikdami savo paslaugas, tiekimo grandinių kibernetinio saugumo;

b) politiką dėl su kibernetiniu saugumu susijusių reikalavimų, taikomų IRT produktams ir IRT paslaugoms, įtraukimo ir specifikacijų viešuosiuose pirkimuose, įskaitant reikalavimus, susijusius su kibernetinio saugumo sertifikavimu, šifravimu ir atvirojo kodo kibernetinio saugumo produktų naudojimu;

c) pažeidžiamumų valdymo, apimančio koordinuoto pažeidžiamumų atskleidimo pagal 12 straipsnio 1 dalį skatinimą ir palengvinimą, politiką;

d) politiką, susijusią su bendru atvirojo interneto viešojo pagrindo prieinamumu, vientisumu ir konfidencialumu, įskaitant, kai tinkama, povandeninių ryšių kabelių kibernetinį saugumą;

e) atitinkamų pažangių technologijų, kuriomis siekiama įgyvendinti pažangiausias kibernetinio saugumo rizikos valdymo priemones, kūrimo ir integravimo skatinimo politiką;

f) švietimo ir mokymo kibernetinio saugumo klausimais, kibernetinio saugumo įgūdžių, informuotumo didinimo ir mokslinių tyrimų ir technologinės plėtros iniciatyvų, taip pat gerosios kibernetinės higienos praktikos ir kontrolės gairių, skirtų piliečiams, suinteresuotiesiems subjektams ir kitiems subjektams, skatinimo ir plėtros politiką;

g) politiką dėl akademinių ir mokslinių tyrimų institucijų rėmimo siekiant kurti, tobulinti ir diegti kibernetinio saugumo priemones ir saugią tinklų infrastruktūrą;

h) politiką, įskaitant atitinkamas procedūras ir tinkamas dalijimosi informacija priemones, siekiant remti savanorišką dalijimąsi kibernetinio saugumo informacija tarp subjektų laikantis Sąjungos teisės;

i) politiką, kuria stiprinami mažųjų ir vidutinių įmonių, visų pirma į šios direktyvos taikymo sritį nepatenkančių įmonių, kibernetinis atsparumas ir kibernetinės higienos bazinis lygis teikiant lengvai prieinamas gaires ir pagalbą jų konkretiems poreikiams tenkinti;

j) politiką, kuria skatinama aktyvi kibernetinė apsauga.

3. Valstybės narės per tris mėnesius nuo savo nacionalinių kibernetinio saugumo strategijų priėmimo apie jas praneša Komisijai. Valstybės narės į tokius pranešimus gali neįtraukti informacijos, kuri susijusi su jų nacionaliniu saugumu.

4. Valstybės narės, remdamosi pagrindiniais veiklos rezultatų rodikliais, reguliariai ir bent kas penkerius metus vertina savo nacionalines kibernetinio saugumo strategijas ir prireikus jas atnaujina. ENISA valstybių narių prašymu padeda joms parengti arba atnaujinti nacionalinę kibernetinio saugumo strategiją ir pagrindinius veiklos rezultatų rodiklius, skirtus tai strategijai įvertinti, siekiant ją suderinti su šioje direktyvoje nustatytais reikalavimais ir pareigomis.

8 straipsnis

Kompetentingos institucijos ir bendrieji kontaktiniai punktai

1. Kiekviena valstybė narė paskiria arba įsteigia vieną arba daugiau kompetentingų institucijų, atsakingų už kibernetinį saugumą ir VII skyriuje nustatytų priežiūros užduočių vykdymą (toliau – kompetentingos institucijos).

2. 1 dalyje nurodytos kompetentingos institucijos stebi šios direktyvos įgyvendinimą nacionaliniu lygmeniu.

3. Kiekviena valstybė narė paskiria arba įsteigia bendrąjį kontaktinį punktą. Kai valstybė narė pagal 1 dalį paskiria arba įsteigia tik vieną kompetentingą instituciją, ta kompetentinga institucija taip pat laikoma tos valstybės narės bendruoju kontaktiniu punktu.

4. Kiekvienas bendras kontaktinis punktas vykdo ryšių palaikymo funkciją, kad būtų užtikrintas jo valstybės narės institucijų tarpvalstybinis bendradarbiavimas su atitinkamomis kitų valstybių narių institucijomis ir, kai tinkama, Komisija bei ENISA, taip pat tarpsektorinis bendradarbiavimas su kitomis kompetentingomis institucijomis toje valstybėje narėje.

5. Valstybės narės užtikrina, kad jų kompetentingos institucijos ir bendrieji kontaktiniai punktai turėtų tinkamų išteklių, kad veiksmingai ir efektyviai vykdytų jiems pavestas užduotis ir taip įgyvendintų šios direktyvos tikslus.

6. Kiekviena valstybė narė nepagrįstai nedelsdama praneša Komisijai 1 dalyje nurodytos kompetentingos institucijos ir 3 dalyje nurodyto bendrojo kontaktinio punkto tapatybės duomenis, tų institucijų užduotis ir bet kokius vėlesnius jų pakeitimus. Kiekviena valstybė narė savo kompetentingos institucijos tapatybės duomenis paskelbia viešai. Komisija viešai paskelbia paskirtų bendrųjų kontaktinių punktų sąrašą.

9 straipsnis

Nacionalinės kibernetinių krizių valdymo sistemos

1. Kiekviena valstybė narė paskiria arba įsteigia vieną arba daugiau kompetentingų institucijų, kurios atsako už didelio masto kibernetinio saugumo incidentų ir krizių valdymą (toliau – kibernetinių krizių valdymo institucijos). Valstybės narės užtikrina, kad tos institucijos turėtų tinkamų išteklių, reikalingų veiksmingam ir efektyviam joms pavestų užduočių vykdymui. Valstybės narės užtikrina suderinamumą su esamomis nacionalinėmis bendro krizių valdymo sistemomis.

2. Jeigu valstybė narė paskiria arba įsteigia pagal 1 dalį daugiau nei vieną kibernetinių krizių valdymo instituciją, ji aiškiai nurodo, kuri iš tų institucijų yra koordinatorė valdant didelio masto kibernetinio saugumo incidentus ir krizes.

3. Kiekviena valstybė narė, taikydama šią direktyvą, nustato pajėgumus, objektus ir procedūras, kuriais galima pasinaudoti krizės atveju.

4. Kiekviena valstybė narė priima nacionalinį reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planą, kuriame išdėstomi didelio masto kibernetinio saugumo incidentų ir krizių valdymo tikslai ir tvarka. Tame plane visų pirma nustatomi:

a) nacionalinių pasirengimo priemonių ir veiksmų tikslai;

b) kibernetinių krizių valdymo institucijų užduotys ir pareigos;

c) kibernetinių krizių valdymo procedūros, įskaitant jų integravimą į nacionalinę bendro krizių valdymo sistemą, ir keitimosi informacija kanalai;

d) nacionalinės pasirengimo priemonės, įskaitant pratybas ir mokymo veiklą;

e) atitinkami viešieji ir privatieji suinteresuotieji subjektai ir naudojama infrastruktūra;

f) atitinkamų nacionalinių institucijų ir įstaigų nacionalinės procedūros ir susitarimai, kuriais siekiama užtikrinti, kad valstybė narė veiksmingai dalyvautų vykdant koordinuotą didelio masto kibernetinio saugumo incidentų ir krizių valdymą Sąjungos lygmeniu ir jį remtų.

5. Per tris mėnesius nuo 1 dalyje nurodytos kibernetinių krizių valdymo institucijos paskyrimo arba įsteigimo kiekviena valstybė narė praneša Komisijai apie savo institucijos tapatybės duomenis ir apie visus vėlesnius jos pakeitimus. Valstybės narės pateikia Komisijai ir Europos ryšių palaikymo dėl kibernetinių krizių organizacinio tinklui (EU-CyCLONe) atitinkamą informaciją, susijusią su 4 dalies reikalavimais, apie savo nacionalinius reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planus per tris mėnesius nuo tų planų priėmimo. Valstybės narės gali nenurodyti konkrečios informacijos, jeigu tai yra būtina jų nacionaliniam saugumui ir tik tokiam saugumui būtinu mastu.

10 straipsnis

Reagavimo į kompiuterių saugumo incidentus tarnybos (CSIRT)

1. Kiekviena valstybė narė paskiria arba įsteigia vieną arba daugiau CSIRT. CSIRT gali būti paskirtos arba įsteigtos kompetentingoje institucijoje. CSIRT laikosi 11 straipsnio 1 dalyje išdėstytų reikalavimų, apima bent I ir II prieduose nurodytus sektorius, subsektorius ir subjektų rūšis ir atsako už incidentų valdymą pagal aiškiai apibrėžtą procesą.

2. Valstybės narės užtikrina, kad kiekviena CSIRT turėtų tinkamų išteklių, kad galėtų veiksmingai vykdyti savo užduotis, nurodytas 11 straipsnio 3 dalyje.

3. Valstybės narės užtikrina, kad kiekviena CSIRT turėtų tinkamą, saugią ir atsparią ryšių ir informacinę struktūrą, kuria naudodamosi jos galėtų keistis informacija su esminiais ir svarbiais subjektais ir kitais atitinkamais suinteresuotaisiais subjektais. Tuo tikslu valstybės narės užtikrina, kad kiekviena CSIRT prisidėtų prie saugaus dalijimosi informacija priemonių diegimo.

4. CSIRT pagal 29 straipsnį bendradarbiauja ir, kai tinkama, keičiasi atitinkama informacija su sektoriaus arba kelių sektorių esminių ir svarbių subjektų bendruomenėmis.

5. CSIRT dalyvauja tarpusavio vertinimuose, kurie organizuojami pagal 19 straipsnį.

6. Valstybės narės užtikrina efektyvų, veiksmingą ir saugų jų CSIRT bendradarbiavimą CSIRT tinkle.

7. CSIRT gali užmegzti bendradarbiavimo ryšius su trečiųjų valstybių nacionalinėmis reagavimo į kompiuterių saugumo incidentus grupėmis. Palaikydamos tokius bendradarbiavimo santykius, valstybės narės sudaro palankesnes sąlygas veiksmingai, efektyviai ir saugiai keistis informacija su tomis trečiųjų valstybių nacionalinėmis reagavimo į kompiuterių saugumo incidentus grupėmis, naudodamos atitinkamus dalijimosi informacija protokolus, įskaitant Srauto kontrolės protokolą. CSIRT gali keistis atitinkama informacija su trečiųjų valstybių nacionalinėmis reagavimo į kompiuterių saugumo incidentus grupėmis, įskaitant asmens duomenis, laikydamosi Sąjungos duomenų apsaugos teisės.

8. CSIRT gali bendradarbiauti su trečiųjų valstybių nacionalinėmis reagavimo į kompiuterių saugumo incidentus grupėmis arba lygiavertėmis trečiųjų valstybių įstaigomis, visų pirma siekdamos teikti joms pagalbą kibernetinio saugumo srityje.

9. Kiekviena valstybė narė nepagrįstai nedelsdama praneša Komisijai šio straipsnio 1 dalyje nurodytos CSIRT ir CSIRT, paskirtos koordinatore pagal 12 straipsnio 1 dalį, tapatybės duomenis, jų atitinkamas užduotis, kurias jos vykdo esminių ir svarbių subjektų atžvilgiu, ir bet kokius vėlesnius jų pakeitimus.

10. Valstybės narės gali paprašyti ENISA padėti kurti jų CSIRT.

11 straipsnis

CSIRT keliami reikalavimai, techniniai pajėgumai ir užduotys

1. CSIRT turi atitikti šiuos reikalavimus:

a) CSIRT užtikrina, kad jų ryšio kanalai būtų lengvai prieinami išvengiant kritinių funkcionavimo trikties taškų, taip pat nustato keletą būdų, kaip bet kuriuo metu susisiekti su jomis ir su kitais subjektais; jos aiškiai nurodo ryšių kanalus ir apie juos informuoja savo klientus ir bendradarbiavimo partnerius;

b) CSIRT biurai ir pagalbinės informacinės sistemos turi būti saugiose vietose;

c) CSIRT aprūpinamos tinkama prašymų valdymo ir nukreipimo sistema, visų pirma siekiant palengvinti veiksmingą ir efektyvų perdavimą;

d) CSIRT užtikrina savo veiklos konfidencialumą ir patikimumą;

e) CSIRT turi turėti pakankamai darbuotojų, kad būtų užtikrintas pasiekiamumas bet kuriuo metu, ir jos turi užtikrinti tinkamą savo darbuotojų mokymą;

f) CSIRT aprūpinamos antrinėmis sistemomis ir atsargine darbo erdve, kad būtų užtikrintas jų paslaugų tęstinumas;

CSIRT gali dalyvauti tarptautiniuose bendradarbiavimo tinkluose.

2. Valstybės narės užtikrina, kad jų CSIRT bendrai turėtų techninių pajėgumų, būtinų, kad galėtų veiksmingai vykdyti savo užduotis, nurodytas 3 dalyje. Valstybės narės užtikrina, kad CSIRT būtų skirta pakankamai išteklių siekiant užtikrinti tinkamą darbuotojų skaičių, kad CSIRT galėtų plėtoti savo techninius pajėgumus.

3. CSIRT vykdo šias užduotis:

a) stebi ir analizuoja kibernetines grėsmes, pažeidžiamumus ir incidentus nacionaliniu lygmeniu, ir, gavusios prašymą, teikia pagalbą atitinkamiems esminiams ir svarbiems subjektams, susijusią su jų tinklų ir informacinių sistemų stebėjimu tikruoju laiku arba beveik tikruoju laiku;

b) teikia ankstyvuosius perspėjimus, įspėjimus, pranešimus ir platina informaciją apie kibernetines grėsmes, pažeidžiamumus ir incidentus esminiams ir svarbiems subjektams, taip pat kompetentingoms institucijoms ir kitiems atitinkamiems suinteresuotiesiems subjektams, jei įmanoma, beveik tikruoju laiku;

c) reaguoja į incidentus ir, kai tikslinga, teikia pagalbą atitinkamiems esminiams ir svarbiems subjektams;

d) renka ir analizuoja teismo ekspertizės duomenis ir teikia dinaminę rizikos bei incidentų analizę, taip pat užtikrina informuotumą apie padėtį kibernetinio saugumo srityje;

e) esminio ar svarbaus subjekto prašymu aktyviai tikrina atitinkamo subjekto tinklų ir informacines sistemas, kad būtų galima atskleisti pažeidžiamumus, galinčius daryti didelį poveikį;

f) dalyvauja CSIRT tinkle ir teikia savitarpio pagalbą pagal savo pajėgumus ir kompetenciją kitiems CSIRT tinklo nariams jų prašymu;

g) kai taikytina, atlieka koordinatoriaus funkcijas koordinuoto pažeidžiamumo atskleidimo tikslais pagal 12 straipsnio 1 dalį;

h) prisideda prie saugaus dalijimosi informacija priemonių diegimo pagal 10 straipsnio 3 dalį.

CSIRT gali atlikti aktyvų neintervencinį esminių ir svarbių subjektų viešai prieinamų tinklų ir informacinių sistemų tikrinimą. Toks tikrinimas atliekamas siekiant aptikti pažeidžiamas arba nesaugiai sukonfigūruotas tinklų ir informacines sistemas ir informuoti atitinkamus subjektus. Toks tikrinimas nedaro jokio neigiamo poveikio subjektų paslaugų veikimui.

Vykdydamos pirmoje pastraipoje nurodytas užduotis, CSIRT gali teikti pirmenybę konkrečioms užduotims remdamosi rizika grindžiamu požiūriu.

4. CSIRT užmezga bendradarbiavimo ryšius su atitinkamais privačiojo sektoriaus suinteresuotaisiais subjektais, kad būtų pasiekti šios direktyvos tikslai.

5. Siekdamos palengvinti bendradarbiavimą, nurodytą 4 dalyje, CSIRT skatina priimti ir naudoti bendrą arba standartizuotą praktiką, klasifikavimo sistemas ir taksonomiją srityse, susijusiose su:

a) incidentų valdymo procedūromis;

b) krizių valdymu ir

c) koordinuotu pažeidžiamumų atskleidimu pagal 12 straipsnio 1 dalį.

12 straipsnis

Koordinuotas pažeidžiamumų atskleidimas ir Europos pažeidžiamumų duomenų bazė

1. Kiekviena valstybė narė paskiria vieną iš savo CSIRT koordinuoto pažeidžiamumų atskleidimo koordinatore. Koordinatore paskirta CSIRT veikia kaip patikimas tarpininkas, prireikus lengvinantis sąveiką tarp pranešimą apie pažeidžiamumą teikiančio fizinio ar juridinio asmens ir gamintojo arba potencialiai pažeidžiamų IRT produktų ar IRT paslaugų teikėjo bet kurios šalies prašymu. Koordinatore paskirtos CSIRT užduotys apima:

a) atitinkamų subjektų nustatymą ir susisiekimą su jais;

b) pagalbos teikimą pranešimus apie pažeidžiamumą teikiantiems fiziniams ar juridiniams asmenims ir

c) derybas dėl informacijos atskleidimo terminų ir pažeidžiamumų, kurie daro poveikį keliems subjektams, valdymą.

Valstybės narės užtikrina, kad fiziniai ar juridiniai asmenys, jei jie to prašo, galėtų anonimiškai pranešti koordinatore paskirtai CSIRT apie pažeidžiamumą. Koordinatore paskirta CSIRT užtikrina, kad būtų imtasi kruopščių tolesnių veiksmų dėl pažeidžiamumo, apie kurį pranešta, ir užtikrina fizinio ar juridinio asmens, teikiančio pranešimą apie pažeidžiamumą, anonimiškumą. Jeigu pažeidžiamumas, apie kurį pranešta, galėtų daryti didelį poveikį subjektams daugiau nei vienoje valstybėje narėje, kiekvienos susijusios valstybės narės koordinatore paskirta CSIRT, kai tinkama, CSIRT tinkle bendradarbiauja su kitomis koordinatorėmis paskirtomis CSIRT.

2. ENISA, pasikonsultavusi su Bendradarbiavimo grupe, sukuria ir tvarko Europos pažeidžiamumų duomenų bazę. Tuo tikslu ENISA sukuria ir tvarko tinkamas informacines sistemas, politiką ir procedūras ir priima Europos pažeidžiamumų duomenų bazės saugumui ir vientisumui užtikrinti būtinas technines ir organizacines priemones, visų pirma siekdama sudaryti sąlygas subjektams, nepriklausomai nuo to, ar jie patenka į šios direktyvos taikymo sritį, bei jų tinklų ir informacinių sistemų tiekėjams, savanoriškai atskleisti ir registruoti viešai žinomas IRT produktų ar IRT paslaugų pažeidžiamumus. Visiems suinteresuotiesiems subjektams suteikiama prieiga prie Europos pažeidžiamumų duomenų bazėje esančios informacijos apie pažeidžiamumus. Toje duomenų bazėje pateikiama:

a) informacija, kuria apibūdinamas pažeidžiamumas;

b) paveikti IRT produktai ar IRT paslaugos ir pažeidžiamumų rimtumas, atsižvelgiant į aplinkybes, kuriomis juo gali būti pasinaudota;

c) informacija apie susijusių pataisų prieinamumą ir, jei pataisų nėra, pažeidžiamų IRT produktų ir IRT paslaugų naudotojams skirtos kompetentingų institucijų arba CSIRT pateiktos gairės, kaip galima sumažinti dėl atskleistų pažeidžiamumų kylančią riziką.

13 straipsnis

Bendradarbiavimas nacionaliniu lygmeniu

1. Kai tos pačios valstybės narės kompetentingos institucijos, bendrasis kontaktinis punktas ir CSIRT yra atskiri, jie bendradarbiauja tarpusavyje, kad vykdytų šioje direktyvoje nustatytas pareigas.

2. Valstybės narės užtikrina, kad jų CSIRT arba, kai taikytina, kompetentingos institucijos gautų pranešimus apie didelius incidentus pagal 23 straipsnį ir incidentus, dideles kibernetines grėsmes ir vos neįvykusius incidentus pagal 30 straipsnį.

3. Valstybės narės užtikrina, kad jų CSIRT arba, kai taikytina, kompetentingos institucijos informuotų savo bendruosius kontaktinius punktus apie šioje direktyvoje nustatyta tvarka pateikiamus pranešimus apie incidentus, kibernetines grėsmes ir vos neįvykusius incidentus.

4. Siekiant užtikrinti, kad kompetentingų institucijų, bendrųjų kontaktinių punktų ir CSIRT užduotys ir pareigos būtų vykdomos veiksmingai, valstybės narės užtikrina tinkamą tų įstaigų ir teisėsaugos institucijų, duomenų apsaugos institucijų, nacionalinių institucijų pagal reglamentus (EB) Nr. 300/2008 ir (ES) 2018/1139, priežiūros įstaigų pagal Reglamentą (ES) Nr. 910/2014, kompetentingų institucijų pagal Reglamentą (ES) 2022/2554, nacionalinių reguliavimo institucijų pagal Direktyvą (ES) 2018/1972, kompetentingų institucijų pagal Direktyvą (ES) 2022/2557, taip pat kompetentingų institucijų pagal kitus konkretiems sektoriams taikomus Sąjungos teisės aktus bendradarbiavimą toje valstybėje narėje.

5. Valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą ir jų kompetentingos institucijos pagal Direktyvą (ES) 2022/2557 bendradarbiautų ir reguliariai keistųsi informacija, kiek tai susiję su ypatingos svarbos subjektų identifikavimu, apie riziką, kibernetines grėsmes, ir incidentus, taip pat apie nekibernetinę riziką, grėsmes ir incidentus, darančius poveikį subjektams, kurie pagal Direktyvą (ES) 2022/2557 identifikuoti kaip ypatingos svarbos subjektai, ir apie priemones, kurių imtasi reaguojant į tą riziką, grėsmes ir incidentus. Valstybės narės taip pat užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą ir jų kompetentingos institucijos pagal Reglamentą (ES) Nr. 910/2014, Reglamentą (ES) 2022/2554 ir Direktyvą (ES) 2018/1972 reguliariai keistųsi atitinkama informacija, be kita ko, susijusia su atitinkamais incidentais ir kibernetinėmis grėsmėmis.

6. Valstybės narės techninėmis priemonėmis supaprastina informacijos, susijusios su 23 ir 30 straipsniuose nurodytais pranešimais, teikimą.

III SKYRIUS

BENDRADARBIAVIMAS SĄJUNGOS IR TARPTAUTINIU LYGMENIMIS

14 straipsnis

Bendradarbiavimo grupė

1. Siekiant remti ir palengvinti strateginį bendradarbiavimą ir keitimąsi informacija tarp valstybių narių, taip pat sustiprinti pasitikėjimą ir patikimumą, sudaroma Bendradarbiavimo grupė.

2. Bendradarbiavimo grupė vykdo savo užduotis remdamasi dvimetėmis darbo programomis, nurodytomis 7 dalyje.

3. Bendradarbiavimo grupę sudaro valstybių narių, Komisijos ir ENISA atstovai. Europos išorės veiksmų tarnyba Bendradarbiavimo grupėje dalyvauja stebėtojos teisėmis. Europos priežiūros institucijos (EPI) ir kompetentingos institucijos pagal Reglamentą (ES) 2022/2554 gali dalyvauti Bendradarbiavimo grupės veikloje pagal to reglamento 47 straipsnio 1 dalį.

Prireikus Bendradarbiavimo grupė gali pakviesti Europos Parlamentą ir atitinkamų suinteresuotųjų subjektų atstovus dalyvauti jos darbe.

Komisija teikia sekretoriato paslaugas.

4. Bendradarbiavimo grupė vykdo šias užduotis:

a) teikia kompetentingoms institucijoms gaires dėl šios direktyvos perkėlimo į nacionalinę teisę ir įgyvendinimo;

b) teikia kompetentingoms institucijoms gaires, susijusias su koordinuoto pažeidžiamumų atskleidimo politikos plėtojimu ir įgyvendinimu, kaip nurodyta 7 straipsnio 2 dalies c punkte;

c) keičiasi geriausios praktikos pavyzdžiais ir informacija, susijusia su šios direktyvos įgyvendinimu, įskaitant informaciją, susijusią su kibernetinėmis grėsmėmis, incidentais, pažeidžiamumais, vos neįvykusiais incidentais, informuotumo didinimo iniciatyvomis, mokymu, pratybomis ir įgūdžiais, gebėjimų stiprinimu, standartais ir techninėmis specifikacijomis, taip pat su esminių ir svarbių subjektų identifikavimu pagal 2 straipsnio 2 dalies b–e punktus;

d) keičiasi patarimais ir bendradarbiauja su Komisija dėl naujų kibernetinio saugumo politikos iniciatyvų ir bendro konkretiems sektoriams taikomų kibernetinio saugumo reikalavimų nuoseklumo;

e) keičiasi patarimais ir bendradarbiauja su Komisija dėl deleguotųjų arba įgyvendinimo aktų, priimamų pagal šią direktyvą, projektų;

f) keičiasi geriausios praktikos pavyzdžiais ir informacija su atitinkamomis Sąjungos institucijomis, įstaigomis, organais ir agentūromis;

g) keičiasi nuomonėmis dėl konkretiems sektoriams taikomų Sąjungos teisės aktų, kuriuose yra nuostatų dėl kibernetinio saugumo, įgyvendinimo;

h) kai tinkama, aptaria 19 straipsnio 9 dalyje nurodytas tarpusavio vertinimo ataskaitas ir parengia išvadas ir rekomendacijas;

i) atlieka koordinuojamus ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimus pagal 22 straipsnio 1 dalį;

j) aptaria savitarpio pagalbos atvejus, įskaitant patirtį ir rezultatus, susijusius su bendrais tarpvalstybiniais priežiūros veiksmais, kaip nurodyta 37 straipsnyje;

k) vienos ar daugiau atitinkamų valstybių narių prašymu aptaria konkrečius savitarpio pagalbos prašymus, nurodytus 37 straipsnyje;

l) teikia strategines gaires CSIRT tinklui ir EU–CyCLONe konkrečiais kylančiais klausimais;

m) keičiasi nuomonėmis dėl politikos dėl tolesnių veiksmų po didelio masto kibernetinio saugumo incidentų ir krizių remiantis CSIRT tinklo ir EU-CyCLONe patirtimi;

n) prisideda prie kibernetinio saugumo pajėgumų visoje Sąjungoje palengvindama nacionalinių pareigūnų mainus pagal gebėjimų stiprinimo programą, kurioje dalyvauja kompetentingų institucijų arba CSIRT darbuotojai;

o) organizuoja nuolatinius bendrus susitikimus su atitinkamais privačiais suinteresuotaisiais subjektais iš visos Sąjungos, kad aptartų Bendradarbiavimo grupės vykdomą veiklą ir surinktų informacijos apie naujus politikos uždavinius;

p) aptaria su kibernetinio saugumo pratybomis susijusį darbą, įskaitant ENISA atliktą darbą;

q) nustato 19 straipsnio 1 dalyje nurodytų tarpusavio vertinimų metodiką ir organizacinius aspektus, taip pat, padedant Komisijai ir ENISA, pagal 19 straipsnio 5 dalį nustato valstybėms narėms savęs vertinimo metodiką, ir, bendradarbiaudama su Komisija ir ENISA, parengia elgesio kodeksus, kuriais grindžiami pagal 19 straipsnio 6 dalį paskirtų kibernetinio saugumo ekspertų darbo metodai;

r) 40 straipsnyje nurodytos peržiūros tikslais rengia Komisijai strateginiu lygmeniu ir atliekant tarpusavio vertinimus sukauptos patirties ataskaitas;

s) aptaria ir reguliariai vertina kibernetinių grėsmių ar incidentų, pavyzdžiui, susijusių su išpirkos reikalavimo programine įranga, padėtį.

Bendradarbiavimo grupė teikia pirmos pastraipos r punkte nurodytas ataskaitas Komisijai, Europos Parlamentui ir Tarybai.

5. Valstybės narės užtikrina efektyvų, veiksmingą ir saugų savo atstovų Bendradarbiavimo grupėje bendradarbiavimą.

6. Bendradarbiavimo grupė gali prašyti, kad CSIRT tinklas parengtų techninę ataskaitą pasirinktomis temomis.

7. Ne vėliau kaip 2024 m. vasario 1 d., o vėliau – kas dvejus metus Bendradarbiavimo grupė parengia darbo programą, skirtą veiksmams, kurių reikia imtis jos tikslams ir užduotims įgyvendinti.

8. Komisija gali priimti įgyvendinimo aktus, kuriais nustatoma procedūrinė tvarka, būtina Bendradarbiavimo grupės veikimui užtikrinti.

Tie įgyvendinimo aktai priimami laikantis 39 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

Komisija keičiasi rekomendacijomis ir bendradarbiauja su Bendradarbiavimo grupe dėl šios dalies pirmoje pastraipoje nurodytų įgyvendinimo aktų projektų pagal 4 dalies e punktą.

9. Bendradarbiavimo grupė nuolat ir ne rečiau kaip kartą per metus susitinka su Ypatingos svarbos subjektų atsparumo klausimų grupe, sudaryta pagal Direktyvą (ES) 2022/2557, kad skatintų ir palengvintų strateginį bendradarbiavimą ir keitimąsi informacija.

15 straipsnis

CSIRT tinklas

1. Siekiant prisidėti prie pasitikėjimo ir atsakomybės didinimo, taip pat skatinti greitą ir veiksmingą valstybių narių operatyvinį bendradarbiavimą, sukuriamas nacionalinių CSIRT tinklas.

2. CSIRT tinklą sudaro pagal 10 straipsnį paskirtų arba įsteigtų CSIRT ir Sąjungos institucijų, įstaigų ir agentūrų kompiuterinių incidentų tyrimo tarnybos (CERT-EU) atstovai. Komisija dalyvauja CSIRT tinklo veikloje stebėtojos teisėmis. ENISA teikia sekretoriato paslaugas ir aktyviai teikia pagalbą CSIRT tarpusavio bendradarbiavimo srityje.

3. CSIRT tinklas vykdo šias užduotis:

a) keičiasi informacija apie CSIRT pajėgumus;

b) padeda CSIRT tarpusavyje dalytis technologijomis ir atitinkamomis priemonėmis, politika, įrankiais, procesais, geriausios praktikos pavyzdžiais ir sistemomis ir juos perduoti bei jais keistis;

c) keičiasi svarbia informacija apie incidentus, vos neįvykusius incidentus, kibernetines grėsmes, riziką ir pažeidžiamumus;

d) keičiasi informacija apie kibernetinio saugumo leidinius ir rekomendacijas;

e) užtikrina sąveikumą, susijusį su dalijimosi informacija specifikacijomis ir protokolais;

f) CSIRT tinklo, kuris galėjo būti paveiktas incidento, nario prašymu keičiasi informacija, susijusia su tuo incidentu ir atitinkamomis kibernetinėmis grėsmėmis, rizika ir pažeidžiamumais, ir ją aptaria;

g) CSIRT tinklo nario prašymu aptaria ir, kai įmanoma, įgyvendina koordinuotą atsaką į incidentą, nustatytą tos valstybės narės jurisdikcijoje;

h) teikia valstybėms narėms pagalbą šalinant tarpvalstybinius incidentus pagal šią direktyvą;

i) bendradarbiauja, keičiasi geriausios praktikos pavyzdžiais ir teikia pagalbą pagal 12 straipsnio 1 dalį koordinatorėmis paskirtoms CSIRT, kiek tai susiję su koordinuoto pažeidžiamumų, galinčių daryti didelį poveikį subjektams daugiau nei vienoje valstybėje narėje, atskleidimo valdymu;

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

   i) kibernetinių grėsmių ir incidentų kategorijomis;

   ii) ankstyvaisiais perspėjimais;

   iii) savitarpio pagalba;

   iv) koordinavimo principais ir tvarka reaguojant į tarpvalstybinę riziką ir incidentus;

   v) pagalba rengiant nacionalinį reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planą, nurodytą 9 straipsnio 4 dalyje, teikiama valstybės narės prašymu;

k) informuoja Bendradarbiavimo grupę apie savo veiklą ir tolesnes operatyvinio bendradarbiavimo formas, aptartas pagal j punktą, ir prireikus prašo tuo klausimu pateikti rekomendacijų;

l) įvertina kibernetinio saugumo pratybas, įskaitant ENISA organizuojamas pratybas;

m) atskiros CSIRT prašymu aptaria tos CSIRT pajėgumus ir parengtį;

n) bendradarbiauja ir keičiasi informacija su regioniniais ir Sąjungos lygmens saugumo operacijų centrais (SOC), kad pagerintų bendrą informuotumą apie padėtį, susijusią su incidentais ir grėsmėmis visoje Sąjungoje;

o) kai tinkama, aptaria 19 straipsnio 9 dalyje nurodytas tarpusavio vertinimo ataskaitas;

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

4. Ne vėliau kaip 2025 m. sausio 17 d., o vėliau – kas dvejus metus CSIRT tinklas 40 straipsnyje nurodytos priežiūros tikslais įvertina padarytą pažangą operatyvinio bendradarbiavimo srityje ir patvirtina ataskaitą. Ataskaitoje visų pirma pateikiamos išvados ir rekomendacijos, grindžiamos 19 straipsnyje nurodytų tarpusavio vertinimų, atliktų dėl nacionalinių CSIRT, rezultatais. Ta ataskaita pateikiama Bendradarbiavimo grupei.

5. CSIRT tinklas priima savo darbo tvarkos taisykles.

6. CSIRT tinklas ir EU-CyCLONe susitaria dėl procedūrinės tvarkos ir ja remdamiesi bendradarbiauja.

16 straipsnis

Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas (EU-CyCLONe)

1. Siekiant remti koordinuotą didelio masto kibernetinio saugumo incidentų ir krizių valdymą operatyviniu lygmeniu ir užtikrinti reguliarų keitimąsi svarbia informacija tarp valstybių narių ir Sąjungos institucijų, įstaigų, organų ir agentūrų, įsteigiamas EU-CyCLONe.

2. EU-CyCLONe sudaro valstybių narių kibernetinių krizių valdymo institucijų atstovai, taip pat tais atvejais, kai galimas arba vykstantis didelio masto kibernetinio saugumo incidentas turi arba gali turėti didelį poveikį paslaugoms ir veiklai, kurioms taikoma ši direktyva – Komisijos atstovai. Kitais atvejais Komisija dalyvauja EU-CyCLONe veikloje stebėtojo teisėmis.

ENISA teikia EU-CyCLONe sekretoriato paslaugas ir padeda saugiai keistis informacija, taip pat teikia būtinas priemones valstybių narių tarpusavio bendradarbiavimui remti, užtikrinančias saugų keitimąsi informacija.

Kai tikslinga, EU-CyCLONe gali pakviesti atitinkamų suinteresuotųjų subjektų atstovus dalyvauti jo darbe stebėtojų teisėmis.

3. EU-CyCLONe vykdo šias užduotis:

a) didina pasirengimo valdyti didelio masto kibernetinio saugumo incidentus ir krizes lygį;

b) plėtoja bendrą informuotumą apie padėtį, susijusią su didelio masto kibernetinio saugumo incidentais ir krizėmis;

c) įvertina atitinkamų didelio masto kibernetinio saugumo incidentų pasekmes ir poveikį ir siūlo galimas švelninimo priemones;

d) koordinuoja didelio masto kibernetinio saugumo incidentų ir krizių valdymą ir padeda politiniu lygmeniu priimti sprendimus, susijusius su tokiais incidentais ir krizėmis;

e) atitinkamos valstybės narės prašymu aptaria 9 straipsnio 4 dalyje nurodytus nacionalinius reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planus.

4. EU-CyCLONe priima savo darbo tvarkos taisykles.

5. EU-CyCLONe reguliariai teikia ataskaitas Bendradarbiavimo grupei apie didelio masto kibernetinio saugumo incidentų ir krizių valdymą, taip pat apie tendencijas, ypatingą dėmesį skirdamas jų poveikiui esminiams ir svarbiems subjektams.

6. EU-CyCLONe su CSIRT tinklu bendradarbiauja remdamasis sutartomis procedūrinėmis taisyklėmis, numatytomis 15 straipsnio 6 dalyje.

7. Ne vėliau kaip 2024 m. liepos 17 d., o vėliau – kas 18 mėnesių EU-CyCLONe teikia Europos Parlamentui ir Tarybai savo darbo įvertinimo ataskaitą.

17 straipsnis

Tarptautinis bendradarbiavimas

Pagal SESV 218 straipsnį Sąjunga, kai tinkama, gali sudaryti tarptautinius susitarimus su trečiosiomis valstybėmis ar tarptautinėmis organizacijomis, pagal kuriuos joms būtų leidžiama dalyvauti tam tikroje Bendradarbiavimo grupės, CSIRT tinklo ir EU-CyCLONe veikloje ir toks dalyvavimas būtų organizuojamas. Tokie susitarimai turi atitikti Sąjungos duomenų apsaugos teisės aktus.

18 straipsnis

Kibernetinio saugumo būklės Sąjungoje ataskaita

1. ENISA, bendradarbiaudama su Komisija ir Bendradarbiavimo grupe, kas dvejus metus patvirtina kibernetinio saugumo Sąjungoje būklės ataskaitą ir tą ataskaitą pateikia ir pristato Europos Parlamentui. Ataskaita, *inter alia*, paskelbiama kaip kompiuterio skaitomi duomenys ir į ją turi būti įtraukti šie aspektai:

a) Sąjungos lygmens kibernetinio saugumo rizikos vertinimas, kuriame atsižvelgiama į kibernetinių grėsmių padėtį;

b) kibernetinio saugumo pajėgumų plėtojimo viešajame ir privačiajame sektoriuose visoje Sąjungoje vertinimas;

c) piliečių ir subjektų, įskaitant mažąsias ir vidutines įmones, bendro informuotumo apie kibernetinį saugumą ir kibernetinės higienos lygio vertinimas;

d) 19 straipsnyje nurodytų tarpusavio vertinimų rezultatų apibendrintas vertinimas;

e) apibendrintas kibernetinio saugumo pajėgumų ir išteklių brandos lygio visoje Sąjungoje, be kita ko, sektorių lygmeniu, taip pat valstybių narių nacionalinių kibernetinio saugumo strategijų suderinimo masto vertinimas.

2. Ataskaitoje pateikiamos konkrečios politikos rekomendacijos, kaip pašalinti trūkumus ir padidinti kibernetinio saugumo lygį visoje Sąjungoje, ir konkretaus laikotarpio išvadų santrauka iš agentūros ES kibernetinio saugumo techninės padėties ataskaitų dėl incidentų ir kibernetinių grėsmių, kurias pagal Reglamento (ES) 2019/881 7 straipsnio 6 dalį parengė ENISA.

3. ENISA, bendradarbiaudama su Komisija, Bendradarbiavimo grupe ir CSIRT tinklu, parengia metodiką, į kurią būtų įtraukiami atitinkami 1 dalies e punkte nurodyto apibendrinto vertinimo kintamieji, pavyzdžiui, kiekybiniai ir kokybiniai rodikliai.

19 straipsnis

Tarpusavio vertinimai

1. Bendradarbiavimo grupė, padedant Komisijai ir ENISA bei, kai tinkama, CSIRT, ne vėliau kaip 2025 m. sausio 17 d. nustato tarpusavio vertinimų metodiką ir organizacinius aspektus, kad būtų galima pasimokyti iš bendros patirties, stiprinti tarpusavio pasitikėjimą, pasiekti aukštą bendrą kibernetinio saugumo lygį, taip pat stiprinti valstybių narių kibernetinio saugumo pajėgumus ir politiką, būtinus šiai direktyvai įgyvendinti. Dalyvavimas tarpusavio vertinimuose yra savanoriškas. Tarpusavio vertinimus atlieka kibernetinio saugumo ekspertai. Kibernetinio saugumo ekspertus skiria bent dvi valstybės narės, kurios nėra vertinamosios valstybės narės.

Tarpusavio vertinimai apima bent vieną iš šių aspektų:

a) kibernetinio saugumo rizikos valdymo priemonių ir pareigų pranešti, įtvirtintų 21 ir 23 straipsniuose, įgyvendinimo lygį;

b) gebėjimų lygį, įskaitant turimus finansinius, techninius ir žmogiškuosius išteklius, ir kompetentingų institucijų užduočių vykdymo veiksmingumą;

c) CSIRT operatyvinius pajėgumus;

d) 37 straipsnyje nurodytos savitarpio pagalbos įgyvendinimo lygį;

e) 29 straipsnyje nurodytų keitimosi kibernetinio saugumo informacija susitarimų įgyvendinimo lygį;

f) konkrečius tarpvalstybinio arba tarpsektorinio pobūdžio klausimus.

2. 1 dalyje nurodyta metodika apima objektyvius, nediskriminacinius, sąžiningus ir skaidrius kriterijus, kuriais remdamosi valstybės narės paskiria kibernetinio saugumo ekspertus, atitinkančius reikalavimus tarpusavio vertinimui atlikti. Komisija ir ENISA dalyvauja tarpusavio vertinimuose stebėtojų teisėmis.

3. Valstybės narės gali nustatyti konkrečius 1 dalies f punkte nurodytus klausimus tarpusavio vertinimui.

4. Prieš pradėdamos 1 dalyje nurodytą tarpusavio vertinimą, valstybės narės praneša dalyvaujančioms valstybėms narėms jo apimtį, įskaitant konkrečius klausimus, nustatytus pagal 3 dalį.

5. Prieš pradėdamos tarpusavio vertinimą, valstybės narės gali pačios įvertinti vertinamus aspektus ir pateikti tą įsivertinimą paskirtiems kibernetinio saugumo ekspertams. Bendradarbiavimo grupė, padedant Komisijai ir ENISA, nustato valstybių narių įsivertinimo metodiką.

6. Tarpusavio vertinimai apima fizinius arba virtualius apsilankymus vietoje ir keitimąsi informacija ne vietoje. Laikantis gero bendradarbiavimo principo, valstybės narės, kurioms taikomas tarpusavio vertinimas, pateikia paskirtiems kibernetinio saugumo ekspertams vertinimui atlikti reikalingą informaciją; tai daroma nedarant poveikio Sąjungos ar nacionalinei teisei dėl konfidencialios ar įslaptintos informacijos apsaugos ir esminių valstybės funkcijų, pavyzdžiui, nacionalinio saugumo, apsaugai. Bendradarbiavimo grupė, bendradarbiaudama su Komisija ir ENISA, parengia atitinkamus elgesio kodeksus, kuriais grindžiami paskirtų kibernetinio saugumo ekspertų darbo metodai. Visa per tarpusavio vertinimą gauta informacija naudojama tik tam vertinimui. Tarpusavio vertinime dalyvaujantys kibernetinio saugumo ekspertai neatskleidžia jokios per tą tarpusavio vertinimą gautos neskelbtinos ar konfidencialios informacijos jokioms trečiosioms šalims.

7. Atlikus tarpusavio vertinimą, tų pačių valstybėje narėje peržiūrėtų aspektų tolesnis tarpusavio vertinimas toje valstybėje narėje dvejus metus po tarpusavio vertinimo pabaigos neatliekamas, nebent valstybė narė prašytų arba Bendradarbiavimo grupei pasiūlius būtų susitarta kitaip.

8. Valstybės narės užtikrina, kad bet kokia su paskirtais kibernetinio saugumo ekspertais susijusi interesų konflikto rizika būtų atskleista kitoms valstybėms narėms, Bendradarbiavimo grupei, Komisijai ir ENISA prieš pradedant tarpusavio vertinimą. Valstybė narė, kuriai taikomas tarpusavio vertinimas, gali dėl tinkamai pagrįstų priežasčių, apie kurias pranešta paskiriančiai valstybei narei, paprieštarauti tam, kad būtų paskirti konkretūs kibernetinio saugumo ekspertai.

9. Tarpusavio vertinimuose dalyvaujantys kibernetinio saugumo ekspertai parengia per tarpusavio vertinimus nustatytų faktų ir išvadų ataskaitas. Valstybės narės, kurioms taikomas tarpusavio vertinimas, gali teikti pastabas dėl su jomis susijusių ataskaitų projektų ir tokios pastabos pridedamos prie ataskaitų. Ataskaitose pateikiamos rekomendacijos, kaip pagerinti aspektus, kuriuos apėmė tarpusavio vertinimas. Kai tinkama, ataskaitos pateikiamos Bendradarbiavimo grupei ir CSIRT tinklui. Valstybė narė, kuriai taikomas tarpusavio vertinimas, gali nuspręsti savo ataskaitą arba jos redaguotą versiją padaryti viešai prieinamą.

IV SKYRIUS

KIBERNETINIO SAUGUMO RIZIKOS VALDYMO PRIEMONĖS IR PAREIGOS PRANEŠTI

20 straipsnis

Valdymas

1. Valstybės narės užtikrina, kad esminių ir svarbių subjektų valdymo organai patvirtintų kibernetinio saugumo rizikos valdymo priemones, kurių ėmėsi tie subjektai, siekdami laikytis 21 straipsnio, prižiūrėtų jo įgyvendinimą ir galėtų būti patraukti atsakomybėn už tai, kad subjektai pažeidžia tą straipsnį.

Šios dalies taikymu nedaromas poveikis nacionalinės teisės aktams, susijusiems su atsakomybės taisyklėmis, taikomomis viešosioms institucijoms, taip pat valstybės tarnautojų ir renkamų ar paskirtų pareigūnų atsakomybe.

2. Valstybės narės užtikrina, kad esminių ir svarbių subjektų valdymo organų nariai turėtų dalyvauti mokymuose, ir skatina esminius ir svarbius subjektus reguliariai siūlyti panašius mokymus savo darbuotojams, kad jie įgytų pakankamai žinių ir įgūdžių, kad galėtų nustatyti riziką ir įvertinti kibernetinio saugumo rizikos valdymo praktiką bei jos poveikį subjekto teikiamoms paslaugoms.

21 straipsnis

Kibernetinio saugumo rizikos valdymo priemonės

1. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai imtųsi tinkamų ir proporcingų techninių, operatyvinių ir organizacinių priemonių, siekdami valdyti tinklų ir informacinių sistemų, kurias tie subjektai naudoja savo veiklai arba teikdami savo paslaugas, saugumui kylančią riziką ir užkirsti kelią incidentų poveikiui jų paslaugų gavėjams ir kitoms paslaugoms arba juos sumažinti iki minimumo.

Atsižvelgiant į naujausius technikos laimėjimus ir, kai taikytina, atitinkamus Europos ir tarptautinius standartus, taip pat į įgyvendinimo sąnaudas, pirmoje pastraipoje nurodytomis priemonėmis užtikrinamas toks tinklų ir informacinių sistemų saugumo lygis, kuris atitinka kilusią riziką. Vertinant tų priemonių proporcingumą, tinkamai atsižvelgiama į subjekto galimybės patirti riziką laipsnį, subjekto dydį ir incidentų tikimybę bei jų sunkumą, įskaitant jų socialinį ir ekonominį poveikį.

2. 1 dalyje nurodytos priemonės grindžiamos visus pavojus apimančiu požiūriu, kuriuo siekiama apsaugoti tinklų ir informacines sistemas bei jų fizinę aplinką nuo incidentų, ir jos apima bent šiuos elementus:

a) rizikos analizės ir informacinių sistemų saugumo politiką;

b) incidentų valdymą;

c) veiklos tęstinumą, pvz., atsarginių kopijų valdymą ir veiklos atkūrimą po ekstremaliųjų įvykių, ir krizių valdymą;

d) tiekimo grandinės saugumą, įskaitant su saugumu susijusius aspektus, susijusius su kiekvieno subjekto ir jo tiesioginių tiekėjų ar paslaugų teikėjų santykiais;

e) tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumą, įskaitant pažeidžiamumo valdymą ir atskleidimą;

f) politiką ir procedūras, skirtas kibernetinio saugumo rizikos valdymo priemonių veiksmingumui įvertinti;

g) pagrindinę kibernetinės higienos praktiką ir kibernetinio saugumo mokymus;

h) kriptografijos ir, kai taikytina, šifravimo naudojimo politiką ir procedūras;

i) žmogiškųjų išteklių saugumą, prieigos kontrolės politiką ir turto valdymą;

j) kai taikytina, kelių veiksnių tapatumo nustatymo ar nuolatinio tapatumo nustatymo sprendimų, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių ryšių sistemų subjekto viduje naudojimą.

3. Valstybės narės užtikrina, kad, subjektai, svarstydami, kurios šio straipsnio 2 dalies d punkte nurodytos priemonės yra tinkamos, atsižvelgtų į kiekvieno tiesioginio tiekėjo ir paslaugų teikėjo pažeidžiamumą ir į jų tiekėjų ir paslaugų teikėjų produktų bendrą kokybę ir kibernetinio saugumo praktiką, įskaitant jų saugumo plėtojimo procedūras. Valstybės narės taip pat užtikrina, kad subjektai, svarstydami, kurios tame punkte nurodytos priemonės yra tinkamos, privalėtų atsižvelgti į pagal 22 straipsnio 1 dalį atliktų koordinuojamų ypatingos svarbos tiekimo grandinių rizikos vertinimų rezultatus.

4. Valstybės narės užtikrina, kad subjektas, kuris nustato, kad jis nesilaiko 2 dalyje numatytų priemonių, nepagrįstai nedelsdamas imtųsi visų būtinų, tinkamų ir proporcingų taisomųjų priemonių.

5. Komisija ne vėliau kaip 2024 m. spalio 17 d. priima įgyvendinimo aktus, kuriais nustatomi 2 dalyje nurodytų priemonių techniniai ir metodiniai reikalavimai, taikomi DNS paslaugų teikėjams, aukščiausio lygio domenų vardų registrams, debesijos kompiuterijos paslaugų teikėjams, duomenų centrų paslaugų teikėjams, turinio teikimo tinklo teikėjams, valdomų paslaugų teikėjams, valdomų saugumo paslaugų teikėjams, elektroninių prekyviečių, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų ir patikimumo užtikrinimo paslaugų teikėjams.

Komisija gali priimti įgyvendinimo aktus, kuriais nustatomi 2 dalyje nurodytų priemonių būtinieji techniniai ir metodiniai reikalavimai, taip pat sektoriams taikomi reikalavimai, taikomi kitiems esminiams ir svarbiems subjektams nei nurodytieji šios dalies pirmoje pastraipoje.

Rengdama šios dalies pirmoje ir antroje pastraipose nurodytus įgyvendinimo aktus, Komisija, kiek įmanoma, laikosi Europos ir tarptautinių standartų bei atitinkamų techninių specifikacijų. Komisija keičiasi rekomendacijomis ir bendradarbiauja su Bendradarbiavimo grupe ir ENISA dėl įgyvendinimo aktų projektų pagal 14 straipsnio 4 dalies e punktą.

Tie įgyvendinimo aktai priimami laikantis 39 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

22 straipsnis

Sąjungos lygmeniu koordinuojami ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimai

1. Bendradarbiavimo grupė, bendradarbiaudama su Komisija ir ENISA, gali atlikti koordinuotus konkrečių ypatingos svarbos IRT paslaugų, IRT sistemų ar IRT produktų tiekimo grandinių saugumo rizikos vertinimus, atsižvelgdama į techninius ir, kai tinkama, netechninius rizikos veiksnius.

2. Komisija, pasikonsultavusi su Bendradarbiavimo grupe ir ENISA bei prireikus su atitinkamais suinteresuotaisiais subjektais, nustato konkrečias ypatingos svarbos IRT paslaugas, IRT sistemas ar IRT produktus, dėl kurių gali būti atliekamas 1 dalyje nurodytas koordinuotas saugumo rizikos vertinimas.

23 straipsnis

Pareigos pranešti

1. Kiekviena valstybė narė užtikrina, kad esminiai ir svarbūs subjektai nepagrįstai nedelsdami praneštų valstybės narės CSIRT arba, kai taikytina, jos kompetentingai institucijai pagal 4 dalį apie bet kokį incidentą, darantį didelį poveikį jų paslaugų teikimui, kaip nurodyta 3 dalyje (toliau – didelis incidentas). Kai tinkama, atitinkami subjektai nepagrįstai nedelsdami praneša jų paslaugų gavėjams apie didelius incidentus, kurie gali turėti neigiamos įtakos tų paslaugų teikimui. Kiekviena valstybė narė užtikrina, kad tie subjektai, *inter alia*, praneštų visą informaciją, pagal kurią CSIRT arba, kai taikytina, kompetentinga institucija galėtų nustatyti tarpvalstybinį incidento poveikį. Vien dėl pranešimo veiksmo negali būti padidinama pranešančiojo subjekto atsakomybė.

Jei atitinkami subjektai praneša kompetentingai institucijai apie didelį incidentą pagal pirmą pastraipą, valstybė narė užtikrina, kad ta kompetentinga institucija, gavusi pranešimą, perduotų jį CSIRT.

Tarpvalstybinio arba tarpsektorinio didelio incidento atveju valstybės narės užtikrina, kad jų bendrieji kontaktiniai punktai laiku gautų atitinkamą informaciją, apie kurią pranešta pagal 4 dalį.

2. Kai taikytina, valstybės narės užtikrina, kad esminiai ir svarbūs subjektai nepagrįstai nedelsdami informuotų savo paslaugų gavėjus, kuriuos didelė kibernetinė grėsmė galėjo paveikti, apie visas priemones ar teisių gynimo priemones, kurių tie gavėjai gali imtis reaguodami į tą grėsmę. Atitinkamais atvejais subjektai taip pat praneša tiems gavėjams apie pačią didelę kibernetinę grėsmę.

3. Incidentas laikomas dideliu, jeigu:

a) dėl jo atitinkamas subjektas patyrė arba gali patirti didelių paslaugų teikimo sutrikimų arba finansinių nuostolių;

b) jis paveikė arba gali paveikti kitus fizinius ar juridinius asmenis sukeldamas didelę turtinę arba neturtinę žalą.

4. Valstybės narės užtikrina, kad 1 dalyje nurodyto pranešimo tikslais atitinkami subjektai CSIRT arba, kai taikytina, kompetentingai institucijai pateiktų:

a) nepagrįstai nedelsdami ir bet kuriuo atveju per 24 valandas nuo tada, kai sužinojo apie didelį incidentą, – ankstyvąjį perspėjimą, kuriame, kai taikytina, nurodoma, ar didelį incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai ir ar jis galėtų daryti tarpvalstybinį poveikį;

b) nepagrįstai nedelsdami ir bet kuriuo atveju per 72 valandas nuo tada, kai sužinojo apie didelį incidentą, – pranešimą apie incidentą, kuriame, kai taikytina, atnaujinama a) punkte nurodyta informacija ir nurodomas didelio incidento, įskaitant jo sunkumą ir poveikį, pradinis vertinimas, taip pat nurodomi užvaldymo rodikliai, jei tokių yra;

c) CSIRT arba, kai taikytina, kompetentingos institucijos prašymu – tarpinę ataskaitą apie atitinkamus atnaujintus duomenis apie padėtį;

d) ne vėliau kaip per vieną mėnesį nuo b punkte nurodyto pranešimo apie incidentą – galutinę ataskaitą, kurioje pateikiama ši informacija:

   i) išsamus incidento, įskaitant jo sunkumą ir poveikį, aprašymas;

   ii) grėsmės arba pagrindinės priežasties, dėl kurios incidentas galėjo būti sukeltas, rūšis;

   iii) taikomos ir įgyvendinamos poveikio mažinimo priemonės;

   iv) kai taikytina, tarpvalstybinis incidento poveikis;

e) tuo atveju, jei d punkte nurodytos galutinės ataskaitos pateikimo metu incidentas tebevyksta, valstybės narės užtikrina, kad atitinkami subjektai tuo metu pateiktų pažangos ataskaitą, o galutinę ataskaitą – per vieną mėnesį nuo tada, kai suvaldė incidentą.

Nukrypstant nuo pirmos pastraipos b punkto, patikimumo užtikrinimo paslaugų teikėjas didelių incidentų, darančių poveikį jo patikimumo užtikrinimo paslaugų teikimui, atveju nepagrįstai nedelsdamas ir bet kuriuo atveju per 24 valandas nuo tada, kai sužinojo apie didelį incidentą, apie tai praneša CSIRT arba, kai taikytina, kompetentingai institucijai.

5. CSIRT arba kompetentinga institucija nepagrįstai nedelsdama ir, kai įmanoma, – per 24 valandas nuo 4 dalies a punkte nurodyto ankstyvojo perspėjimo gavimo pateikia atsakymą pranešančiajam subjektui, įskaitant pirminę grįžtamąją informaciją apie didelį incidentą, ir, subjekto prašymu – galimų rizikos mažinimo priemonių įgyvendinimo gaires arba operacinių patarimų. Jei CSIRT nėra pradinis 1 dalyje nurodyto pranešimo gavėjas, gaires teikia kompetentinga institucija, bendradarbiaudama su CSIRT. CSIRT teikia papildomą techninę pagalbą, jei to prašo atitinkamas subjektas. Jei įtariama, kad didelis incidentas yra baudžiamojo pobūdžio, CSIRT arba kompetentinga institucija taip pat teikia gaires dėl pranešimo apie didelį incidentą teisėsaugos institucijoms.

6. Kai taikytina ir visų pirma tuomet, kai didelis incidentas yra susijęs su dviem ar daugiau valstybių narių, CSIRT, kompetentinga institucija arba bendrasis kontaktinis punktas nepagrįstai nedelsdami informuoja apie didelį incidentą kitas paveiktas valstybes nares, ir ENISA. Tokia informacija apima pagal 4 dalį gautos informacijos rūšį. Tai darydami CSIRT, kompetentinga institucija ar bendrasis kontaktinis punktas, laikydamiesi Sąjungos arba nacionalinės teisės, saugo subjekto saugumo ir komercinius interesus, taip pat pateiktos informacijos konfidencialumą.

7. Kai visuomenės informuotumas yra būtinas siekiant užkirsti kelią dideliam incidentui ar reaguoti į besitęsiantį didelį incidentą arba kai didelio incidento atskleidimas kitais atvejais atitinka viešąjį interesą, valstybės narės CSIRT arba, kai taikytina, jos kompetentinga institucija ir atitinkamais atvejais kitų atitinkamų valstybių narių CSIRT arba kompetentingos institucijos, gali, pasikonsultavusios su atitinkamu subjektu, informuoti visuomenę apie incidentą arba pareikalauti, kad tą padarytų subjektas.

8. CSIRT arba kompetentingos institucijos prašymu bendrasis kontaktinis punktas perduoda pagal 1 dalį gautus pranešimus kitų paveiktų valstybių narių bendriesiems kontaktiniams punktams.

9. Bendrasis kontaktinis punktas kas tris mėnesius teikia ENISA suvestinę ataskaitą, į kurią įtraukiami nuasmeninti ir suvestiniai duomenys apie didelius incidentus, incidentus, kibernetines grėsmes ir vos neįvykusius incidentus, apie kuriuos pranešta pagal šio straipsnio 1 dalį ir pagal 30 straipsnį. Siekdama prisidėti prie palyginamos informacijos teikimo ENISA gali priimti technines gaires dėl į suvestinę ataskaitą įtrauktos informacijos parametrų. ENISA kas šešis mėnesius informuoja Bendradarbiavimo grupę ir CSIRT tinklą apie savo išvadas dėl gautų pranešimų.

10. CSIRT arba, kai taikytina, kompetentingos institucijos teikia kompetentingoms institucijoms pagal Direktyvą (ES) 2022/2557 informaciją apie didelius incidentus, incidentus, kibernetines grėsmes ir vos neįvykusius incidentus, apie kuriuos pagal šio straipsnio 1 dalį ir 30 straipsnį pranešė subjektai, identifikuoti kaip ypatingos svarbos subjektai pagal Direktyvą (ES) 2022/2557

11. Komisija gali priimti įgyvendinimo aktus, kuriais išsamiau nustatoma pagal šio straipsnio 1 dalį ir 30 straipsnį pateikiamo pranešimo ir pagal šio straipsnio 2 dalį pateikiamos informacijos rūšis, formatas ir procedūra.

Komisija ne vėliau kaip 2024 m. spalio 17 d. priima įgyvendinimo aktus dėl DNS paslaugų teikėjų, aukšto lygio domenų vardų registrų, debesijos kompiuterijos paslaugų teikėjų, duomenų centrų paslaugų teikėjų, turinio teikimo tinklo teikėjų, valdomų paslaugų teikėjų, valdomų saugumo paslaugų teikėjų, taip pat elektroninių prekyviečių, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų teikėjų, kuriais išsamiau apibrėžiami atvejai, kuriais incidentas laikomas dideliu, kaip nurodyta 3 dalyje. Komisija gali priimti tokius įgyvendinimo aktus dėl kitų esminių ir svarbių subjektų.

Komisija keičiasi rekomendacijomis ir bendradarbiauja su Bendradarbiavimo grupe dėl šios dalies pirmoje ir antroje pastraipose nurodytų įgyvendinimo aktų projektų pagal 14 straipsnio 4 dalies e punktą.

Tie įgyvendinimo aktai priimami laikantis 39 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

24 straipsnis

Europos kibernetinio saugumo sertifikavimo schemų naudojimas

1. Siekdamos įrodyti atitiktį tam tikriems 21 straipsnio reikalavimams, valstybės narės gali reikalauti, kad esminiai ir svarbūs subjektai naudotų konkrečius esminių ar svarbių subjektų sukurtus arba iš trečiųjų šalių nupirktus IRT produktus, IRT paslaugas ir IRT procesus, kurie sertifikuoti pagal Europos kibernetinio saugumo sertifikavimo schemas, priimtas pagal Reglamento (ES) 2019/881 49 straipsnį. Be to, valstybės narės skatina esminius ir svarbius subjektus naudotis kvalifikuotomis patikimumo užtikrinimo paslaugomis.

2. Komisijai pagal 38 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, kuriais ši direktyva papildoma nustatant, kokių kategorijų esminiai ir svarbūs subjektai privalo naudoti tam tikrus sertifikuotus IRT produktus, IRT paslaugas ir IRT procesus arba gauti sertifikatą pagal Europos kibernetinio saugumo sertifikavimo schemą, priimtą pagal Reglamento (ES) 2019/881 49 straipsnį. Tie deleguotieji aktai priimami tais atvejais, kai nustatomi nepakankami kibernetinio saugumo lygiai, ir į tuos aktus įtraukiamas įgyvendinimo laikotarpis.

Prieš priimdama tokius deleguotuosius aktus, Komisija atlieka poveikio vertinimą ir vykdo konsultacijas pagal Reglamento (ES) 2019/881 56 straipsnį.

3. Kai šio straipsnio 2 dalies tikslais nėra tinkamos Europos kibernetinio saugumo sertifikavimo schemos, Komisija, pasikonsultavusi su Bendradarbiavimo grupe ir Europos kibernetinio saugumo sertifikavimo grupe, gali prašyti ENISA parengti potencialią schemą pagal Reglamento (ES) 2019/881 48 straipsnio 2 dalį.

25 straipsnis

Standartizacija

1. Siekdamos skatinti vienodą 21 straipsnio 1 ir 2 dalių įgyvendinimą, valstybės narės, nereikalaudamos taikyti kokios nors konkrečios rūšies technologijos ir nesuteikdamos jai pirmenybės, skatina naudotis Europos ir tarptautiniais standartais ir techninėmis specifikacijomis, kurie yra svarbūs tinklų ir informacinių sistemų saugumui.

2. ENISA, bendradarbiaudama su valstybėmis narėmis ir, kai tikslinga, pasikonsultavusi su atitinkamais suinteresuotaisiais subjektais, parengia rekomendacijas ir gaires dėl techninių sričių, kurios turi būti apsvarstytos atsižvelgiant į 1 dalį, taip pat dėl jau galiojančių standartų, be kita ko, nacionalinių standartų, kuriuose būtų numatyta įtraukti tas sritis.

V SKYRIUS

JURISDIKCIJA IR REGISTRACIJA

26 straipsnis

Jurisdikcija ir teritoriškumas

1. Laikoma, kad subjektai, patenkantys į šios direktyvos taikymo sritį, laikomi priklausančiais valstybės narės, kurioje jie yra įsisteigę, jurisdikcijai, išskyrus:

a) viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjus, kurie laikomi priklausančiais valstybės narės, kurioje jie teikia savo paslaugas, jurisdikcijai;

b) DNS paslaugų teikėjus, aukščiausio lygio domenų vardų registrus, domenų vardų registravimo paslaugas teikiančius subjektus, debesijos kompiuterijos paslaugų teikėjus, duomenų centrų paslaugų teikėjus, turinio teikimo tinklo paslaugų teikėjus, valdomų paslaugų teikėjus, valdomų saugumo paslaugų teikėjus, taip pat elektroninių prekyviečių, interneto paieškos sistemų ar socialinio tinklo paslaugų platformų paslaugų teikėjus, kurie laikomi priklausančiais valstybės narės, kurioje yra jų pagrindinė buveinė Sąjungoje, jurisdikcijai;

c) viešojo administravimo subjektus, kurie laikomi priklausančiais valstybės narės, kuri juos įsteigė, jurisdikcijai.

2. Šios direktyvos tikslais laikoma, kad 1 dalies b punkte nurodyto subjekto pagrindinė buveinė Sąjungoje yra valstybėje narėje, kurioje daugiausia priimami su kibernetinio saugumo rizikos valdymo priemonėmis susiję sprendimai. Jei tokios valstybės narės neįmanoma nustatyti arba jei tokie sprendimai nepriimami Sąjungoje, laikoma, kad pagrindinė buveinė yra valstybėje narėje, kurioje vykdomos kibernetinio saugumo operacijos. Jei tokios valstybės narės neįmanoma nustatyti, laikoma, kad pagrindinė buveinė yra valstybėje narėje, kurioje atitinkamas subjektas turi padalinį, kuriame dirba daugiausia darbuotojų Sąjungoje.

3. Jei 1 dalies b punkte nurodytas subjektas nėra įsisteigęs Sąjungoje, bet teikia paslaugas Sąjungoje, jis paskiria atstovą Sąjungoje. Atstovas turi būti įsisteigęs vienoje iš tų valstybių narių, kuriose siūlomos paslaugos. Laikoma, kad toks subjektas priklauso valstybės narės, kurioje yra įsisteigęs jo atstovas, jurisdikcijai. Jei Sąjungoje nėra pagal šią dalį paskirto atstovo, bet kuri valstybė narė, kurioje subjektas teikia paslaugas, gali imtis teisinių veiksmų prieš subjektą dėl šios direktyvos pažeidimo.

4. 1 dalies b punkte nurodyto subjekto atstovo paskyrimu nedaromas poveikis teisiniams veiksmams, kurie galėtų būti inicijuoti prieš patį subjektą.

5. Valstybės narės, gavusios savitarpio pagalbos prašymą dėl 1 dalies b punkte nurodyto subjekto, gali, neviršydamos to prašymo ribų, imtis tinkamų priežiūros ir vykdymo užtikrinimo priemonių, susijusių su atitinkamu subjektu, teikiančiu paslaugas arba turinčiu tinklų ir informacinę sistemą jų teritorijoje.

27 straipsnis

Subjektų registras

1. ENISA sukuria ir tvarko DNS paslaugų teikėjų, aukščiausio lygio domenų vardų registrų, domenų vardų registravimo paslaugas teikiančių subjektų, debesijos kompiuterijos paslaugų teikėjų, duomenų centrų paslaugų teikėjų, turinio teikimo tinklo paslaugų teikėjų, valdomų paslaugų teikėjų, valdomų saugumo paslaugų teikėjų, taip pat internetinių prekyviečių, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų paslaugų teikėjų registrą, remdamasi iš bendrųjų kontaktinių punktų pagal 4 dalį gauta informacija. Gavusi prašymą, ENISA suteikia kompetentingoms institucijoms prieigą prie to registro, kartu, kai taikytina, užtikrindama informacijos konfidencialumo apsaugą.

2. Valstybės narės reikalauja, kad 1 dalyje nurodyti subjektai kompetentingoms institucijoms ne vėliau kaip 2025 m. sausio 17 d. pateiktų šią informaciją:

a) subjekto pavadinimą;

b) I arba II priede nurodytą atitinkamą sektorių, subsektorių ir subjekto rūšį, jei taikoma;

c) subjekto pagrindinės buveinės adresą ir kitus juridinius padalinius Sąjungoje arba, jei jie nėra įsisteigę Sąjungoje, pagal 26 straipsnio 3 dalį paskirto atstovo adresą;

d) naujausius kontaktinius duomenis, įskaitant subjekto ir, kai taikytina, pagal 26 straipsnio 3 dalį paskirto jo atstovo el. pašto adresus ir telefono numerius;

e) valstybes nares, kuriose subjektas teikia paslaugas, ir

f) subjekto IP adresų ruožus.

3. Valstybės narės užtikrina, kad 1 dalyje nurodyti subjektai nedelsdami ir bet kuriuo atveju ne vėliau kaip per tris mėnesius nuo pakeitimo dienos praneštų kompetentingai institucijai apie bet kokius jų pagal 2 dalį pateiktos informacijos pakeitimus.

4. Gavęs 2 ir 3 dalyse nurodytą informaciją, išskyrus 2 dalies f punkte nurodytą informaciją, atitinkamos valstybės narės bendrasis kontaktinis punktas, nepagrįstai nedelsdamas ją persiunčia ENISA.

5. Kai taikytina, šio straipsnio 2 ir 3 dalyse nurodyta informacija teikiama naudojantis 3 straipsnio 4 dalies ketvirtoje pastraipoje nurodytu nacionaliniu mechanizmu.

28 straipsnis

Domenų vardų registracijos duomenų bazė

1. Siekdamos prisidėti prie DNS saugumo, stabilumo ir atsparumo, valstybės narės reikalauja, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai rūpestingai rinktų ir specialioje duomenų bazėje saugotų tikslius ir išsamius domenų vardų registracijos duomenis, laikydamiesi Sąjungos duomenų apsaugos teisės aktų dėl duomenų, kurie yra asmens duomenys.

2. 1 dalies tikslais valstybės narės reikalauja, kad domenų vardų registracijos duomenų bazėse būtų būtina informacija, pagal kurią būtų galima nustatyti domenų vardų turėtojus ir kontaktinius punktus, administruojančius aukščiausio lygio domenų vardais pažymėtus domenų vardus, ir su jais susisiekti. Tokia informacija apima:

a) domeno vardą;

b) registracijos datą;

c) registruotojo pavadinimą, pavardę, kontaktinį el. pašto adresą ir telefono numerį;

d) domeno vardą administruojančio kontaktinio punkto el. pašto adresą ir telefono numerį, jei jie skiriasi nuo registruotojo duomenų.

3. Valstybės narės reikalauja, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai taikytų politiką ir procedūras, įskaitant tikrinimo procedūras, kuriomis užtikrinama, kad 1 dalyje nurodytose duomenų bazėse būtų pateikiama tiksli ir išsami informacija. Valstybės narės reikalauja, kad tokia politika ir procedūros būtų skelbiamos viešai.

4. Valstybės narės reikalauja, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai nepagrįstai nedelsdami po domeno vardo užregistravimo viešai paskelbtų domeno vardo registracijos duomenis, kurie nėra asmens duomenys.

5. Valstybės narės reikalauja, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai, gavę teisėtus ir tinkamai pagrįstus teisėtų prieigos prašančių subjektų prašymus, suteiktų prieigą prie konkrečių domenų vardų registracijos duomenų, laikydamiesi Sąjungos duomenų apsaugos teisės aktų. Valstybės narės reikalauja, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai, atsakytų nepagrįstai nedelsdami ir bet kuriuo atveju per 72 valandas nuo tada, kai gaunamas prašymas suteikti prieigą. Valstybės narės reikalauja, kad tokių duomenų atskleidimo politika ir procedūros būtų skelbiamos viešai.

6. Dėl to, kad laikomasi 1–5 dalyse nustatytų pareigų, neturi būti dubliuojamas domenų vardų registracijos duomenų rinkimas. Tuo tikslu valstybės narės reikalauja, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai bendradarbiautų tarpusavyje.

VI SKYRIUS

DALIJIMASIS INFORMACIJA

29 straipsnis

Dalijimosi kibernetinio saugumo informacija susitarimai

1. Valstybės narės užtikrina, kad subjektai, patenkantys į šios direktyvos taikymo sritį, ir, kai tinkama, kiti subjektai, nepatenkantys į šios direktyvos taikymo sritį, galėtų savanoriškai tarpusavyje keistis svarbia kibernetinio saugumo informacija, įskaitant informaciją, susijusią su kibernetinėmis grėsmėmis, vos neįvykusiais incidentais, pažeidžiamumais, metodais ir procedūromis, užvaldymo rodikliais, priešiška taktika, konkrečių grėsmių ir dalyvių informacija, kibernetinio saugumo įspėjimais ir rekomendacijomis dėl kibernetinio saugumo priemonių konfigūracijos siekiant aptikti kibernetinius išpuolius, kai tokiu dalijimusi informacija:

a) siekiama užkirsti kelią incidentams, juos atskleisti, į juos reaguoti ar po jų atstatyti veiklą, arba sumažinti jų poveikį;

b) didinamas kibernetinis saugumas, visų pirma didinant informuotumą apie kibernetines grėsmes, ribojant arba sustabdant tokių grėsmių plitimo galimybes, remiant įvairius gynybos pajėgumus, pažeidžiamumų ištaisymą ir atskleidimą, grėsmių nustatymo, sustabdymo ir prevencijos metodus, švelninimo strategijas ar reagavimo ir veiklos atstatymo etapus, arba skatinant viešųjų ir privačiųjų subjektų atliekamus bendradarbiavimu grindžiamus kibernetinių grėsmių mokslinius tyrimus.

2. Valstybės narės užtikrina, kad informacija būtų keičiamasi esminių ir svarbių subjektų ir, kai tinkama, jų tiekėjų ar paslaugų teikėjų bendruomenėse. Toks keitimasis vykdomas taikant dalijimosi kibernetinio saugumo informacija susitarimus, susijusius su galimai neskelbtina informacija, kuria dalijamasi.

3. Valstybės narės sudaro palankesnes sąlygas sudaryti šio straipsnio 2 dalyje nurodytus dalijimosi kibernetinio saugumo informacija susitarimus. Tokiuose susitarimuose gali būti nustatyti veiklos elementai, įskaitant specialių IT platformų ir automatizavimo priemonių naudojimą, dalijimosi informacija susitarimų turinys ir sąlygos. Nustatydamos išsamią informaciją apie valdžios institucijų dalyvavimą tokiuose susitarimuose, valstybės narės gali nustatyti sąlygas dėl informacijos, kurią turi pateikti kompetentingos institucijos arba CSIRT. Valstybės narės teikia pagalbą tokių susitarimų taikymui pagal 7 straipsnio 2 dalies h punkte nurodytą savo politiką.

4. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai kompetentingoms institucijoms praneša apie savo dalyvavimą 2 dalyje nurodytuose dalijimosi informacija susitarimuose sudarydami tokius susitarimus arba, kai tinkama, apie pasitraukimą iš tokių susitarimų, kai toks pasitraukimas įsigalioja.

5. ENISA teikia pagalbą sudarant 2 dalyje nurodytų dalijimosi kibernetinio saugumo informacija susitarimus, teikdama geriausios praktikos pavyzdžius ir gaires.

30 straipsnis

Savanoriškas pranešimas apie svarbią informaciją

1. Valstybės narės užtikrina, kad, be 23 straipsnyje numatytos pranešimų teikimo pareigos, pranešimus CSIRT arba, kai taikytina, kompetentingoms institucijoms, savanoriškai galėtų teikti:

a) esminiai ir svarbūs subjektai apie incidentus, kibernetines grėsmes ir vos neįvykusius incidentus;

b) kiti nei a punkte nurodyti subjektai, nepriklausomai nuo to, ar jie patenka į šios direktyvos taikymo sritį – apie didelius incidentus, kibernetines grėsmes ir vos neįvykusius incidentus.

2. Valstybės narės tvarko šio straipsnio 1 dalyje nurodytus pranešimus laikydamosi procedūros, nustatytos 23 straipsnyje. Valstybės narės gali teikti pirmenybę privalomų pranešimų tvarkymui, palyginti su savanoriškais pranešimais.

Prireikus CSIRT ir, kai taikytina, kompetentingos institucijos teikia bendriesiems kontaktiniams punktams informaciją apie pagal šį straipsnį gautus pranešimus, kartu užtikrindamos pranešimą teikiančio subjekto pateiktos informacijos konfidencialumą ir tinkamą apsaugą. Nedarant poveikio nusikalstamų veikų prevencijai, tyrimui, jų atskleidimui ir baudžiamajam persekiojimui už jas, dėl savanoriško pranešimo pranešimą teikiančiam subjektui nenustatoma jokių papildomų pareigų, kurios jam nebūtų taikomos, jei jis nebūtų pateikęs pranešimo.

VII SKYRIUS

PRIEŽIŪRA IR VYKDYMO UŽTIKRINIMAS

31 straipsnis

Bendrieji aspektai, susiję su priežiūra ir vykdymo užtikrinimu

1. Valstybės narės užtikrina, kad jų kompetentingos institucijos veiksmingai vykdytų priežiūrą ir imtųsi priemonių, būtinų siekiant užtikrinti, kad būtų laikomasi šios direktyvos.

2. Valstybės narės gali leisti savo kompetentingoms institucijoms nustatyti užduočių prioritetus priežiūros srityje. Prioritetai nustatomi vadovaujantis rizika grindžiamu požiūriu. Tuo tikslu, vykdydamos savo priežiūros užduotis, numatytas 32 ir 33 straipsniuose, kompetentingos institucijos gali nustatyti priežiūros metodikas, pagal kurias būtų galima nustatyti tokių užduočių prioritetus, laikantis rizika grindžiamo požiūrio.

3. Kompetentingos institucijos, nagrinėdamos incidentus, dėl kurių pažeidžiamas asmens duomenų saugumas, glaudžiai bendradarbiauja su priežiūros institucijomis pagal Reglamentą (ES) 2016/679, nedarant poveikio priežiūros institucijų kompetencijai ir užduotims pagal tą reglamentą.

4. Nedarant poveikio nacionalinėms teisėkūros ir institucinėms sistemoms, valstybės narės užtikrina, kad, vykdydamos priežiūrą, kaip viešojo administravimo subjektai laikosi šios direktyvos, ir taikydamos vykdymo užtikrinimo priemones šios direktyvos pažeidimų atveju, kompetentingos institucijos turėtų atitinkamus įgaliojimus vykdyti tokias užduotis naudodamosi veiklos nepriklausomumu nuo prižiūrimų viešojo administravimo subjektų. Valstybės narės gali nuspręsti dėl tinkamų, proporcingų ir veiksmingų priežiūros ir vykdymo užtikrinimo priemonių nustatymo tų subjektų atžvilgiu pagal nacionalines teisines ir institucines sistemas.

32 straipsnis

Esminių subjektų priežiūros ir vykdymo užtikrinimo priemonės

1. Valstybės narės užtikrina, kad priežiūros ar vykdymo užtikrinimo priemonės, taikomos esminiams subjektams šioje direktyvoje nustatytų pareigų atžvilgiu, būtų veiksmingos, proporcingos ir atgrasomos, atsižvelgiant į kiekvieno konkretaus atvejo aplinkybes.

2. Valstybės narės užtikrina, kad kompetentingos institucijos, vykdydamos savo priežiūros užduotis, susijusias su esminiais subjektais, turėtų bent šiuos įgaliojimus taikyti tiems subjektams:

a) atlikti patikrinimus vietoje ir priežiūrą ne vietoje, įskaitant atsitiktinius patikrinimus, kuriuos atlieka apmokyti specialistai;

b) atlikti reguliarius ir tikslinius saugumo auditus, kuriuos vykdo nepriklausoma įstaiga arba kompetentinga institucija;

c) atlikti *ad hoc* auditus, be kita ko, kai tai pateisinama dėl didelio incidento arba esminio subjekto padaryto šios direktyvos pažeidimo atveju;

d) atlikti saugumo patikrinimus, pagrįstus objektyviais, nediskriminaciniais, sąžiningais ir skaidriais rizikos vertinimo kriterijais, bendradarbiaudamos, kai to reikia, su atitinkamu subjektu;

e) prašyti pateikti informaciją, būtiną atitinkamo subjekto priimtoms kibernetinio saugumo rizikos valdymo priemonėms įvertinti, įskaitant dokumentais pagrįstą kibernetinio saugumo politiką, taip pat informacijos teikimo pareigos kompetentingoms institucijoms pagal 27 straipsnį laikymąsi;

f) prašyti leisti susipažinti su duomenimis, dokumentais ir informacija, reikalinga jų priežiūros užduotims atlikti;

g) prašyti pateikti kibernetinio saugumo politikos įgyvendinimo įrodymus, pavyzdžiui, kvalifikuoto auditoriaus atliktų saugumo auditų rezultatus ir atitinkamus pagrindinius įrodymus.

Pirmos pastraipos b punkte nurodyti tiksliniai saugumo auditai grindžiami kompetentingos institucijos arba audituojamo subjekto atliktais rizikos vertinimais arba kita turima su rizika susijusia informacija.

Bet kokio tikslinio saugumo audito rezultatai pateikiami kompetentingai institucijai. Tokio tikslinio saugumo audito, kurį atlieka nepriklausoma įstaiga, išlaidas padengia audituojamas subjektas, išskyrus tinkamai pagrįstus atvejus, kai kompetentinga institucija nusprendžia kitaip.

3. Naudodamosi savo įgaliojimais pagal 2 dalies e, f arba g punktą, kompetentingos institucijos nurodo prašymo tikslą ir tiksliai apibrėžia prašomą informaciją.

4. Valstybės narės užtikrina, kad jų kompetentingos institucijos, naudodamosi savo vykdymo užtikrinimo įgaliojimais esminių subjektų atžvilgiu, turėtų bent šiuos įgaliojimus:

a) teikti įspėjimus, kad atitinkami subjektai pažeidžia šią direktyvą;

b) priimti privalomus nurodymus, įskaitant nurodymus dėl priemonių, kurių reikia siekiant užkirsti kelią incidentui arba jam išspręsti, ir tokių priemonių įgyvendinimo bei ataskaitų apie jų įgyvendinimą terminus, arba įsakymą, kuriuo reikalaujama, kad atitinkami subjektai pašalintų nustatytus trūkumus arba ištaisytų šios direktyvos pažeidimus;

c) nurodyti atitinkamiems subjektams nutraukti veiksmus, kurie pažeidžia šią direktyvą, ir tokių veiksmų nebekartoti;

d) nurodyti atitinkamiems subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų kibernetinio saugumo rizikos valdymo priemonės atitiktų 21 straipsnį arba kad jie įvykdytų 23 straipsnyje nustatytas pareigas pranešti;

e) įpareigoti atitinkamus subjektus informuoti fizinius arba juridinius asmenis, kuriems jie teikia paslaugas arba vykdo veiklą ir kuriuos didelė kibernetinė grėsmė gali paveikti, apie grėsmės pobūdį, taip pat apie visas galimas apsaugos ar taisomąsias priemones, kurių gali imtis tie fiziniai ar juridiniai asmenys, reaguodami į tą grėsmę;

f) įpareigoti atitinkamus subjektus per pagrįstą terminą įgyvendinti saugumo audito metu pateiktas rekomendacijas;

g) paskirti stebėsenos pareigūną, kuriam per nustatytą laikotarpį pavestos aiškiai apibrėžtos užduotys, prižiūrėti, kaip atitinkami subjektai laikosi 21 ir 23 straipsnių;

h) įpareigoti atitinkamus subjektus konkrečiu būdu viešai paskelbti šios direktyvos pažeidimo aspektus;

i) skirti arba prašyti, kad atitinkamos įstaigos ar teismai pagal nacionalinę teisę skirtų administracinę baudą pagal 34 straipsnį, kartu su bet kuriomis šios dalies a–h punktuose nurodytomis priemonėmis.

5. Jei pagal 4 dalies a–d ir f punktus patvirtintos vykdymo užtikrinimo priemonės yra neveiksmingos, valstybės narės užtikrina, kad jų kompetentingos institucijos turėtų įgaliojimus nustatyti terminą, iki kurio esminis subjektas turi imtis būtinų veiksmų trūkumams pašalinti arba tų institucijų reikalavimams įvykdyti. Jei per nustatytą terminą nesiimama prašomų veiksmų, valstybės narės užtikrina, kad jų kompetentingos institucijos turėtų įgaliojimus:

a) laikinai sustabdyti arba prašyti, kad sertifikavimo arba leidimus išduodanti įstaiga, arba teismas pagal nacionalinę teisę laikinai sustabdytų sertifikavimą arba įgaliojimą, susijusį su dalimi arba visomis esminio subjekto teikiamomis atitinkamomis paslaugomis ar vykdoma veikla;

b) reikalauti, kad atitinkamos įstaigos arba teismai pagal nacionalinę teisę nustatytų laikiną draudimą bet kuriam esminiame subjekte generalinio direktoriaus ar teisinio atstovo lygmens vadovaujamas pareigas einančiam fiziniam asmeniui eiti vadovaujamas pareigas tame subjekte.

Laikini sustabdymai arba draudimai, nustatyti pagal šią dalį, taikomi tik tol, kol atitinkamas subjektas nesiims būtinų veiksmų trūkumams pašalinti arba kompetentingos institucijos reikalavimams, dėl kurių taikytos tokios vykdymo užtikrinimo priemonės, įvykdyti. Skiriant tokius laikinus sustabdymus ar draudimus, turi būti taikomos tinkamos procedūrinės apsaugos priemonės pagal bendruosius Sąjungos teisės ir Chartijos principus, įskaitant teisę į veiksmingą teisinę gynybą bei teisingą bylos nagrinėjimą, nekaltumo prezumpciją ir teisę į gynybą.

Šioje dalyje numatytos vykdymo užtikrinimo priemonės netaikomos viešojo administravimo subjektams, kuriems taikoma ši direktyva.

6. Valstybės narės užtikrina, kad fizinis asmuo, atsakingas už esminį subjektą arba veikiantis kaip jo teisinis atstovas, remdamasis jam suteiktais įgaliojimais atstovauti tam subjektui, įgaliojimu priimti sprendimus jo vardu arba įgaliojimu vykdyti jo kontrolę, turėtų įgaliojimus užtikrinti, kad subjektas laikytųsi šios direktyvos. Valstybės narės užtikrina, kad tie fiziniai asmenys galėtų būti traukiami atsakomybėn už jų pareigų užtikrinti šios direktyvos laikymąsi.

Viešojo administravimo subjektų atžvilgiu šia dalimi nedaromas poveikis nacionalinės teisės aktams, susijusiems su valstybės tarnautojų ir renkamų ar paskirtų pareigūnų atsakomybe.

7. Imdamosi bet kurios iš 4 dalyje nurodytų vykdymo užtikrinimo priemonių kompetentingos institucijos gerbia teisę į gynybą ir atsižvelgia į kiekvieno konkretaus atvejo aplinkybes ir tinkamai atsižvelgia bent į:

a) pažeidimo sunkumą ir pažeistų nuostatų svarbą; sunkiais pažeidimais, *inter alia*, bet kuriuo atveju laikomi:

   i) pakartotiniai pažeidimai;

   ii) nepranešimas apie didelius incidentus;

   iii) trūkumų pagal kompetentingų institucijų privalomus vykdyti nurodymus neištaisymas;

   iv) trukdymas vykdyti audito ar stebėsenos veiklą, kurią įpareigojo atlikti kompetentinga institucija nustačius pažeidimą;

   v) neteisingos ar labai netikslios informacijos, susijusios su kibernetinio saugumo rizikos valdymo priemonėmis arba pareigomis pranešti, nustatytomis 21 ir 23 straipsniuose, pateikimas;

b) pažeidimo trukmę;

c) atitinkamo subjekto įvykdytus svarbius ankstesnius pažeidimus;

d) padarytą turtinę arba neturtinę žalą, įskaitant finansinius ar ekonominius nuostolius, poveikį kitoms paslaugoms ir paveiktų naudotojų skaičių;

e) tai, ar pažeidimą įvykdęs asmuo veikė tyčia ar dėl neatsargumo;

f) priemones, kurių subjektas ėmėsi siekdamas užkirsti kelią turtinei ar neturtinei žalai arba ją sumažinti;

g) patvirtintų elgesio kodeksų arba patvirtintų sertifikavimo mechanizmų laikymąsi;

h) atsakingais laikomų fizinių ar juridinių asmenų bendradarbiavimo su kompetentingomis institucijomis lygį.

8. Kompetentingos institucijos išsamiai pagrindžia savo vykdymo užtikrinimo priemones. Prieš priimdamos tokias priemones kompetentingos institucijos atitinkamiems subjektams praneša apie savo preliminarias išvadas. Jos taip pat suteikia tiems subjektams pagrįstą laikotarpį pastaboms pateikti, išskyrus tinkamai pagrįstus atvejus, kai tai trukdytų imtis neatidėliotinų incidentų prevencijos arba reagavimo į juos veiksmų.

9. Valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą informuotų toje pačioje valstybėje narėje esančias atitinkamas kompetentingas institucijas pagal Direktyvą (ES) 2022/2557, kai jos naudojasi savo priežiūros ir vykdymo užtikrinimo įgaliojimais, kuriais siekiama užtikrinti, kad subjektas, kuris pagal Direktyvą (ES) 2022/2557 identifikuotas kaip ypatingos svarbos subjektas, laikytųsi šios direktyvos. Kai taikytina, kompetentingos institucijos pagal Direktyvą (ES) 2022/2557 gali prašyti kompetentingų institucijų pagal šią direktyvą naudotis savo priežiūros ir vykdymo užtikrinimo įgaliojimais subjekto, kuris identifikuojamas kaip ypatingos svarbos subjektas pagal Direktyvą (ES) 2022/2557, atžvilgiu.

10. Valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą bendradarbiautų su atitinkamomis atitinkamos valstybės narės kompetentingomis institucijomis pagal Reglamentą (ES) 2022/2554 Visų pirma valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą informuotų Priežiūros forumą, įsteigtą pagal Reglamento (ES) 2022/2554 32 straipsnio 1 dalį, kai jos naudojasi priežiūros ir vykdymo užtikrinimo įgaliojimais, kuriais siekiama užtikrinti, kad esminis subjektas, paskirtas ypatingai svarbiu trečiųjų šalių IRT paslaugų teikėju pagal Reglamento (ES) 2022/2554 31 straipsnį, laikytųsi šios direktyvos.

33 straipsnis

Svarbių subjektų priežiūros ir jų pareigų vykdymo užtikrinimo priemonės

1. Gavusios įrodymų, duomenų ar informacijos, kad svarbus subjektas, kaip įtariama, nesilaiko šios direktyvos, visų pirma jos 21 ir 23 straipsnių, valstybės narės užtikrina, kad kompetentingos institucijos prireikus imtųsi veiksmų taikydamos *ex post* priežiūros priemones. Valstybės narės užtikrina, kad tos priemonės būtų veiksmingos, proporcingos ir atgrasomos, atsižvelgiant į kiekvieno konkretaus atvejo aplinkybes.

2. Valstybės narės užtikrina, kad kompetentingos institucijos, vykdydamos savo priežiūros užduotis, susijusias su svarbiais subjektais, turėtų bent šiuos įgaliojimus taikyti tiems subjektams:

a) atlikti patikrinimus vietoje ir vykdyti *ex post* priežiūrą ne vietoje, kuriuos atlieka apmokyti specialistai;

b) atlikti tikslinius saugumo auditus, kuriuos vykdo kvalifikuota nepriklausoma įstaiga arba kompetentinga institucija;

c) atlikti saugumo patikrinimus, pagrįstus objektyviais, nediskriminaciniais, sąžiningais ir skaidriais rizikos vertinimo kriterijais, bendradarbiaudamos, kai to reikia, su atitinkamu subjektu;

d) prašyti pateikti informaciją, būtiną atitinkamo subjekto priimtoms kibernetinio saugumo rizikos valdymo priemonėms įvertinti *ex post*, įskaitant dokumentais pagrįstą kibernetinio saugumo politiką, taip pat pareigos teikti informaciją kompetentingoms institucijoms pagal 28 straipsnį laikymąsi;

e) prašyti leisti susipažinti su duomenimis, dokumentais ir informacija, reikalinga priežiūros užduotims atlikti;

f) prašyti pateikti kibernetinio saugumo politikos įgyvendinimo įrodymus, pavyzdžiui, kvalifikuoto auditoriaus atliktų saugumo auditų rezultatus ir atitinkamus pagrindinius įrodymus.

Pirmos pastraipos b punkte nurodyti tiksliniai saugumo auditai grindžiami kompetentingos institucijos arba audituojamo subjekto atliktais rizikos vertinimais arba kita turima su rizika susijusia informacija.

Bet kokio tikslinio saugumo audito rezultatai pateikiami kompetentingai institucijai. Tokio tikslinio saugumo audito, kurį atlieka nepriklausoma įstaiga, išlaidas padengia audituojamas subjektas, išskyrus tinkamai pagrįstus atvejus, kai kompetentinga institucija nusprendžia kitaip.

3. Naudodamosi savo įgaliojimais pagal 2 dalies d, e arba f punktą, kompetentingos institucijos nurodo prašymo tikslą ir patikslina prašomą informaciją.

4. Valstybės narės užtikrina, kad kompetentingos institucijos, naudodamosi savo vykdymo užtikrinimo įgaliojimais svarbių subjektų atžvilgiu, turėtų bent šiuos įgaliojimus:

a) teikti įspėjimus, kad atitinkami subjektai pažeidžia šią direktyvą;

b) priimti privalomus nurodymus arba įsakymą, kuriuo reikalaujama, kad atitinkami subjektai pašalintų nustatytus trūkumus arba ištaisytų šios direktyvos pažeidimą;

c) nurodyti atitinkamiems subjektams nutraukti veiksmus, kurie pažeidžia šią direktyvą, ir tokių veiksmų nebekartoti;

d) nurodyti atitinkamiems subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų kibernetinio saugumo rizikos valdymo priemonės atitiktų 21 straipsnį arba kad jie įvykdytų 23 straipsnyje nustatytas pareigas pranešti;

e) įpareigoti atitinkamus subjektus informuoti fizinius arba juridinius asmenis, kuriems jie teikia paslaugas arba vykdo veiklą ir kuriuos gali paveikti didelė kibernetinė grėsmė, apie grėsmės pobūdį, taip pat apie visas galimas apsaugos ar taisomąsias priemones, kurių gali imtis tie fiziniai ar juridiniai asmenys, reaguodami į tą grėsmę;

f) įpareigoti atitinkamus subjektus per pagrįstą terminą įgyvendinti saugumo audito metu pateiktas rekomendacijas;

g) įpareigoti atitinkamus subjektus konkrečiu būdu viešai paskelbti šios direktyvos pažeidimo aspektus;

h) skirti arba prašyti, kad atitinkamos įstaigos ar teismai pagal nacionalinę teisę skirtų administracinę baudą pagal 34 straipsnį, kartu su bet kuriomis šios dalies a–g punktuose nurodytomis priemonėmis.

5. 32 straipsnio 6, 7 ir 8 dalys *mutatis mutandis* taikomos šiame straipsnyje numatytoms priežiūros ir vykdymo užtikrinimo priemonėms, skirtoms svarbiems subjektams.

6. Valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą bendradarbiautų su atitinkamomis atitinkamos valstybės narės kompetentingomis institucijomis pagal Reglamentą (ES) 2022/2554. Visų pirma valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą informuotų Priežiūros forumą, įsteigtą pagal Reglamento (ES) 2022/2554 32 straipsnio 1 dalį, kai jos naudojasi priežiūros ir vykdymo užtikrinimo įgaliojimais, kuriais siekiama užtikrinti, kad svarbus subjektas, paskirtas ypatingai svarbiu trečiųjų šalių IRT paslaugų teikėju pagal Reglamento (ES) 2022/2554 31 straipsnį, laikytųsi šios direktyvos.

34 straipsnis

Bendrosios administracinių baudų skyrimo esminiams ir svarbiems subjektams sąlygos

1. Valstybės narės užtikrina, kad už šios direktyvos pažeidimus esminiams ir svarbiems subjektams skiriamos administracinės baudos pagal šį straipsnį kiekvienu atskiru atveju būtų veiksmingos, proporcingos ir atgrasomos, atsižvelgiant į kiekvieno konkretaus atvejo aplinkybes.

2. Administracinės baudos skiriamos kartu su 32 straipsnio 4 dalies a–h punktuose, 32 straipsnio 5 dalyje ir 33 straipsnio 4 dalies a–g punktuose nurodytomis priemonėmis.

3. Sprendžiant, ar skirti administracinę baudą, ir kiekvienu konkrečiu atveju priimant sprendimą dėl jos dydžio, deramai atsižvelgiama bent į 32 straipsnio 7 dalyje nurodytus aspektus.

4. Valstybės narės užtikrina, kad už 21 arba 23 straipsnio pažeidimus pagal šio straipsnio 2 ir 3 dalis esminiams subjektams būtų skiriamos administracinės baudos, kurių didžiausia būtų bent 10 000 000 EUR arba kurių didžiausia būtų bent 2 proc. įmonės, kuriai tas esminis subjektas priklauso, bendros pasaulinės metinės apyvartos praėjusiais finansiniais metais, atsižvelgiant į tai, kuri suma yra didesnė.

5. Valstybės narės užtikrina, kad už 21 arba 23 straipsnio pažeidimus pagal šio straipsnio 2 ir 3 dalis svarbiems subjektams būtų skiriamos administracinės baudos, kurių didžiausia būtų bent 7 000 000 EUR arba kurių didžiausia būtų bent 1,4 proc. įmonės, kuriai tas svarbus subjektas priklauso, bendros pasaulinės metinės apyvartos praėjusiais finansiniais metais, atsižvelgiant į tai, kuri suma yra didesnė.

6. Valstybės narės gali numatyti įgaliojimą skirti periodines baudas, siekiant priversti esminį arba svarbų subjektą nutraukti šios direktyvos pažeidimą, remiantis išankstiniu kompetentingos institucijos sprendimu.

7. Nedarant poveikio kompetentingų institucijų įgaliojimams pagal 32 ir 33 straipsnius, kiekviena valstybė narė gali nustatyti taisykles dėl to, ar ir kokiu mastu administracinės baudos gali būti skiriamos viešojo administravimo subjektams, kuriems taikomos šioje direktyvoje nustatytos pareigos.

8. Jei valstybės narės teisės sistemoje nenumatoma administracinių baudų, ta valstybė narė užtikrina, kad šis straipsnis galėtų būti taikomas taip, kad baudą inicijuotų kompetentinga institucija, o ją skirtų kompetentingi nacionaliniai teismai arba specialios jurisdikcijos teismai, sykiu užtikrinant, kad tos teisių gynimo priemonės būtų veiksmingos ir turėtų kompetentingų institucijų skiriamoms administracinėms baudoms lygiavertį poveikį. Bet kuriuo atveju skiriamos baudos turi būti veiksmingos, proporcingos ir atgrasomosios. Valstybė narė ne vėliau kaip 2024 m. spalio 17 d. praneša Komisijai apie įstatymų, kuriuos ji priima pagal šią dalį, nuostatas ir nedelsdama praneša apie visus vėlesnius tas nuostatas keičiančius teisės aktus arba joms įtakos turinčius pakeitimus.

35 straipsnis

Pažeidimai, susiję su asmens duomenų saugumo pažeidimu

1. Jeigu, vykdydamos priežiūrą ar vykdymo užtikrinimą, kompetentingos institucijos išsiaiškina, kad dėl esminio arba svarbaus subjekto padaryto šios direktyvos 21 ir 23 straipsniuose nustatytų pareigų pažeidimo gali būti padarytas asmens duomenų saugumo pažeidimas, kaip apibrėžta Reglamento (ES) 2016/679 4 straipsnio 12 punkte, apie kurį turi būti pranešta pagal to reglamento 33 straipsnį, jos, nepagrįstai nedelsdamos, informuoja priežiūros institucijas, kaip nurodyta to reglamento 55 arba 56 straipsnyje.

2. Jeigu priežiūros institucijos, kaip nurodyta Reglamento (ES) 2016/679 55 arba 56 straipsnyje, skiria administracinę baudą pagal to reglamento 58 straipsnio 2 dalies i punktą, kompetentingos institucijos negali skirti administracinės baudos pagal šios direktyvos 34 straipsnį už šio straipsnio 1 dalyje nurodytą pažeidimą, įvykdytą tuo pačiu elgesiu, už kurį buvo skirta administracinė bauda pagal Reglamento (ES) 2016/679 58 straipsnio 2 dalies i punktą. Tačiau kompetentingos institucijos gali taikyti šios direktyvos 32 straipsnio 4 dalies a–h punktuose, 32 straipsnio 5 dalyje ir 33 straipsnio 4 dalies a–g punktuose numatytas vykdymo užtikrinimo priemones.

3. Jeigu priežiūros institucija, kompetentinga pagal Reglamentą (ES) 2016/679, yra įsteigta kitoje valstybėje narėje nei kompetentinga institucija, kompetentinga institucija apie 1 dalyje nurodytą galimą duomenų pažeidimą informuoja jos pačios valstybėje narėje įsteigtą priežiūros instituciją.

36 straipsnis

Sankcijos

Valstybės narės nustato sankcijų, taikomų pažeidus pagal šią direktyvą priimtas nacionalines nuostatas, taisykles ir imasi visų būtinų priemonių užtikrinti, kad šios sankcijos būtų įgyvendinamos. Numatytos sankcijos turi būti veiksmingos, proporcingos ir atgrasomos. Valstybės narės ne vėliau kaip 2025 m. sausio 17 d. praneša Komisijai apie tas taisykles ir priemones ir nepagrįstai nedelsdamos informuoja ją apie visus vėlesnius joms įtakos turinčius pakeitimus.

37 straipsnis

Savitarpio pagalba

1. Kai subjektas teikia paslaugas daugiau nei vienoje valstybėje narėje arba teikia paslaugas vienoje ar daugiau valstybių narių, o jo tinklų ir informacinės sistemos yra vienoje ar daugiau kitų valstybių narių, atitinkamų valstybių narių kompetentingos institucijos viena su kita bendradarbiauja ir padeda viena kitai. Tas bendradarbiavimas apima bent tai, kad:

a) valstybės narės kompetentingos institucijos, taikančios priežiūros arba vykdymo užtikrinimo priemones, per bendrąjį kontaktinį punktą informuoja kitų atitinkamų valstybių narių kompetentingas institucijas ir su jomis konsultuojasi dėl priežiūros ir vykdymo užtikrinimo priemonių, kurių imtasi;

b) kompetentinga institucija gali prašyti kitos kompetentingos institucijos imtis priežiūros arba vykdymo užtikrinimo priemonių;

c) kompetentinga institucija, gavusi kitos kompetentingos institucijos pagrįstą prašymą, teikia kitai kompetentingai institucijai savitarpio pagalbą, proporcingą jos pačios turimiems ištekliams, kad priežiūros ar vykdymo užtikrinimo priemonės galėtų būti įgyvendinamos veiksmingai, efektyviai ir nuosekliai.

Pirmos pastraipos c punkte nurodyta savitarpio pagalba gali apimti prašymus pateikti informaciją ir priežiūros priemones, įskaitant prašymus atlikti patikrinimus vietoje arba priežiūrą ne vietoje, arba tikslinius saugumo auditus. Kompetentinga institucija, kuriai pateiktas pagalbos prašymas, negali atmesti to prašymo, išskyrus atvejus, kai nustatoma, kad ji neturi kompetencijos teikti prašomą pagalbą, prašoma pagalba nėra proporcinga kompetentingos institucijos priežiūros atliekamų užduočių atžvilgiu arba prašymas yra susijęs su informacija arba apima veiklą, kuri, ją atskleidus arba atlikus, prieštarautų tos valstybės narės nacionaliniam saugumui, visuomenės saugumui ar gynybai. Prieš atsisakydama patenkinti tokį prašymą, kompetentinga institucija konsultuojasi su kitomis atitinkamomis kompetentingomis institucijomis, taip pat, vienos iš atitinkamų valstybių narių prašymu, su Komisija ir ENISA.

2. Kai tinkama ir bendru sutarimu, skirtingų valstybių narių kompetentingos institucijos gali vykdyti bendrus priežiūros veiksmus.

VIII SKYRIUS

DELEGUOTIEJI IR ĮGYVENDINIMO AKTAI

38 straipsnis

Įgaliojimų delegavimas

1. Įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami šiame straipsnyje nustatytomis sąlygomis.

2. 24 straipsnio 2 dalyje nurodyti įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami penkerių metų laikotarpiui nuo 2023 m. sausio 16 d.

3. Europos Parlamentas arba Taryba gali bet kada atšaukti 24 straipsnio 2 dalyje nurodytus deleguotuosius įgaliojimus. Sprendimu dėl įgaliojimų atšaukimo nutraukiami tame sprendime nurodyti įgaliojimai priimti deleguotuosius aktus. Sprendimas įsigalioja kitą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje* arba vėlesnę jame nurodytą dieną. Jis nedaro poveikio jau galiojančių deleguotųjų aktų galiojimui.

4. Prieš priimdama deleguotąjį aktą Komisija konsultuojasi su kiekvienos valstybės narės paskirtais ekspertais vadovaudamasi 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros nustatytais principais.

5. Apie priimtą deleguotąjį aktą Komisija nedelsdama vienu metu praneša Europos Parlamentui ir Tarybai.

6. Pagal 24 straipsnio 2 dalį priimtas deleguotasis aktas įsigalioja tik tuo atveju, jeigu per du mėnesius nuo pranešimo Europos Parlamentui ir Tarybai apie šį aktą dienos nei Europos Parlamentas, nei Taryba nepareiškia prieštaravimų arba jeigu dar nepasibaigus šiam laikotarpiui ir Europos Parlamentas, ir Taryba praneša Komisijai, kad prieštaravimų nereikš. Europos Parlamento arba Tarybos iniciatyva šis laikotarpis pratęsiamas dviem mėnesiais.

39 straipsnis

Komiteto procedūra

1. Komisijai padeda komitetas. Tas komitetas – tai komitetas, kaip tai suprantama Reglamente (ES) Nr. 182/2011.

2. Kai daroma nuoroda į šią dalį, taikomas Reglamento (ES) Nr. 182/2011 5 straipsnis.

3. Kai komiteto nuomonei gauti būtina rašytinė procedūra, tokia procedūra laikoma baigta be rezultato, jei per nuomonei pateikti nustatytą laikotarpį taip nusprendžia komiteto pirmininkas arba to prašo komiteto narys.

IX SKYRIUS

BAIGIAMOSIOS NUOSTATOS

40 straipsnis

Peržiūra

Komisija ne vėliau kaip 2027 m. spalio 17 d. peržiūri šios direktyvos taikymą ir teikia ataskaitą Europos Parlamentui ir Tarybai. Ataskaitoje visų pirma įvertinama susijusių subjektų dydžio ir I ir II prieduose nurodytų sektorių, subsektorių ir subjektų rūšių svarba ekonomikos ir visuomenės veikimui kibernetinio saugumo atžvilgiu. Tuo 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 lygmenimis. Kai būtina, prie ataskaitos pridedamas pasiūlymas dėl teisėkūros procedūra priimamo akto.

41 straipsnis

Perkėlimas į nacionalinės teisės aktus

1. Valstybės narės ne vėliau kaip 2024 m. spalio 17 d., priima ir paskelbia nuostatas, būtinas, kad būtų laikomasi šios direktyvos. Apie tai jos nedelsdamos praneša Komisijai.

Tas nuostatas jos taiko nuo 2024 m. spalio 18 d..

2. Valstybės narės, priimdamos 1 dalyje nurodytas nuostatas, daro jose nuorodą į šią direktyvą arba tokia nuoroda daroma jas oficialiai skelbiant. Nuorodos darymo tvarką nustato valstybės narės.

42 straipsnis

Reglamento (ES) Nr. 910/2014 dalinis pakeitimas

Reglamento (ES) Nr. 910/2014 19 straipsnis išbraukiamas nuo 2024 m. spalio 18 d.

43 straipsnis

Direktyvos (ES) 2018/1972 dalinis pakeitimas

Direktyvos (ES) 2018/1972 40 ir 41 straipsniai išbraukiami nuo 2024 m. spalio 18 d.

44 straipsnis

Panaikinimas

Direktyva (ES) 2016/1148 panaikinama nuo 2024 m. spalio 18 d.

Nuorodos į panaikintą direktyvą laikomos nuorodomis į šią direktyvą ir skaitomos pagal III priede pateiktą atitikties lentelę.

45 straipsnis

Įsigaliojimas

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

46 straipsnis

Adresatai

Ši direktyva skirta valstybėms narėms.

Priimta Strasbūre 2022 m. gruodžio 14 d.

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkė	*Pirmininkas*
R. METSOLA	M. BEK

I PRIEDAS

YPATINGOS SVARBOS SEKTORIAI

Sektorius	Subsektorius	Subjekto rūšis
1. Energetika	a) Elektra	— Elektros energijos įmonės, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2019/944 ([1])2 straipsnio 57 punkte, vykdančios „tiekimo“ funkciją, kaip apibrėžta tos direktyvos 2 straipsnio 12 punkte
		— Skirstymo sistemos operatoriai, kaip apibrėžta Direktyvos (ES) 2019/944 2 straipsnio 29 punkte
		— Perdavimo sistemos operatoriai, kaip apibrėžta Direktyvos (ES) 2019/944 2 straipsnio 35 punkte
		— Gamintojai, kaip apibrėžta Direktyvos (ES) 2019/944 2 straipsnio 38 punkte
		— Paskirtieji elektros energijos rinkos operatoriai, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2019/943 ([2]) 2 straipsnio 8 punkte — Elektros energijos rinkos dalyviai, kaip apibrėžta Reglamento (ES) 2019/943 2 straipsnio 25 punkte, teikiantys telkimo, reguliavimo apkrovos arba energijos kaupimo paslaugas, nurodytas Direktyvos (ES) 2019/944 2 straipsnio 18, 20 ir 59 punktuose — Įkrovimo prieigos operatoriui, atsakingi už įkrovimo prieigos, kuri naudojama įkrovimo paslaugai galutiniams naudotojams teikti, taip pat ir judumo paslaugų teikėjo vardu bei jo pavedimu, valdymą ir eksploatavimą
	b) Centralizuotas šilumos ir vėsumos tiekimas	— Centralizuoto šilumos tiekimo arba centralizuoto vėsumos tiekimo, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2018/2001 ([3])2 straipsnio 19 punkte, operatoriai
	c) Nafta	— Naftotiekių operatoriai
		— Naftos gamybos, perdirbimo ir apdorojimo įrenginių, laikymo ir perdavimo operatoriai
		— Centrinės atsargų saugyklos, kaip apibrėžta Tarybos direktyvos 2009/119/EB ([4])2 straipsnio f punkte
	d) Dujos	— Tiekimo įmonės, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2009/73/EB ([5])2 straipsnio 8 punkte
		— Skirstymo sistemos operatoriai, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 6 punkte
		— Perdavimo sistemos 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
	e) Vandenilis	— Vandenilio gamybos, laikymo ir perdavimo operatoriai

Sektorius	Subsektorius	Subjekto rūšis
2. Transportas	a) Oro transportas	— Oro vežėjai, kaip apibrėžta Reglamento (EB) Nr. 300/2008 3 straipsnio 4 punkte, naudojami komerciniais tikslais
		— Oro uosto valdymo organai, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2009/12/EB ([6])2 straipsnio 2 punkte, oro uostai, kaip apibrėžta tos direktyvos 2 straipsnio 1 punkte, įskaitant Europos Parlamento ir Tarybos reglamento (ES) Nr. 1315/2013 ([7])II priedo 2 skirsnyje išvardytus pagrindinius oro uostus, ir subjektai, eksploatuojantys oro uostuose esančius pagalbinius įrenginius
		— Skrydžių valdymo operatoriai, teikiantys skrydžių valdymo (ATC) paslaugas, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (EB) Nr. 549/2004 ([8])2 straipsnio 1 punkte
	b) Geležinkelių transportas	— Infrastruktūros valdytojai, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2012/34/ES ([9])3 straipsnio 2 punkte
		— Geležinkelio įmonės, kaip apibrėžta Direktyvos 2012/34/ES 3 straipsnio 1 punkte, įskaitant paslaugų įrenginių operatorius, kaip apibrėžta tos direktyvos 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 ([10]) I priede, neįskaitant tų bendrovių eksploatuojamų atskirų laivų
		— Uostų, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2005/65/EB ([11])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 (LET), kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2002/59/EB ([12]) 3 straipsnio o punkte, operatoriai
	d) Kelių transportas	— Kelių direkcijos, kaip apibrėžta Komisijos deleguotojo reglamento (ES) 2015/962 ([13]) 2 straipsnio 12 punkte, atsakingos už eismo valdymo kontrolę, išskyrus viešuosius subjektus, kuriems eismo valdymo arba intelektinių transporto sistemų operatoriaus veikla yra tik neesminė jų bendrosios veiklos dalis
		— Intelektinių transporto sistemų, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2010/40/ES ([14]) 4 straipsnio 1 punkte, operatoriai
3. Bankininkystė		Kredito įstaigos, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) Nr. 575/2013 ([15])4 straipsnio 1 punkte
4. Finansų rinkų infrastruktūros objektai		— Prekybos vietų, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2014/65/ES ([16])4 straipsnio 24 punkte, operatoriai
		— Pagrindinės sandorio šalys (PSŠ), kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) Nr. 648/2012 ([17]) 2 straipsnio 1 punkte

Sektorius	Subsektorius	Subjekto rūšis
5. Sveikatos priežiūra		— Sveikatos priežiūros paslaugų teikėjai, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2011/24/ES ([18])3 straipsnio g punkte
		— ES etaloninės laboratorijos, nurodytos Europos Parlamento ir Tarybos reglamento (ES) 2022/2371 ([19]) 15 straipsnyje
		— Subjektai, vykdantys vaistų, apibrėžtų Europos Parlamento ir Tarybos direktyvos 2001/83/EB ([20])1 straipsnio 2 punkte, mokslinių tyrimų ir kūrimo veiklą — Subjektai, gaminantys pagrindinius farmacijos produktus ir farmacijos preparatus, nurodytus NACE 2 red. C skirsnio 21 skyriuje — Subjektai, gaminantys medicinos priemones, kurios laikomos ypatingos svarbos ekstremaliosios visuomenės sveikatos situacijos atveju (ypatingos svarbos medicinos priemonių ekstremaliosios visuomenės sveikatos situacijos atveju sąrašas), kaip tai suprantama Europos Parlamento ir Tarybos reglamento (ES) 2022/123 ([21]) 22 straipsnyje
6. Geriamasis vanduo		Žmonėms vartoti skirto vandens, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2020/2184 ([22]) 2 straipsnio 1 punkto a papunktyje, tiekėjai ir skirstytojai, išskyrus skirstytojus, kuriems žmonėms vartoti skirto vandens skirstymas yra neesminė jų bendrosios kitų prekių ir produktų paskirstymo veiklos dalis
7. Nuotekos		Miesto nuotekas, buitines nuotekas ir pramonines nuotekas, nurodytas Tarybos direktyvos 91/271/EEB ([23]) 2 straipsnio 1, 2 ir 3 punktuose, renkančios, šalinančios ar valančios įmonės, išskyrus įmones, kurioms miesto nuotekų, buitinių nuotekų ar pramoninių nuotekų rinkimas, šalinimas ar valymas yra neesminė jų bendrosios veiklos dalis
8. Skaitmeninė infrastruktūra		— Interneto duomenų srautų mainų taško teikėjai
		— DNS paslaugų teikėjai, išskyrus šakninio pavadinimo serverių operatorius
		— Aukščiausio lygio domenų vardų registrai
		— Debesijos kompiuterijos paslaugų teikėjai
		— Duomenų centrų paslaugų teikėjai
		— Turinio teikimo tinklo teikėjai
		— Patikimumo užtikrinimo paslaugų teikėjai
		— Viešųjų elektroninių ryšių tinklų teikėjai
		— Viešai prieinamų elektroninių ryšių paslaugų teikėjai
9. IRT paslaugų valdymas (verslas verslui)		— Valdomų paslaugų teikėjai — Valdomų saugumo paslaugų teikėjai

Sektorius	Subsektorius	Subjekto rūšis
10. Viešasis administravimas		— Centrinės valdžios viešojo administravimo subjektai, kaip valstybė narė apibrėžė pagal nacionalinę teisę
		— Regioninio lygmens viešojo administravimo subjektai, kaip valstybė narė apibrėžė pagal nacionalinę teisę
11. Kosmosas		Valstybėms narėms arba privačiosioms šalims priklausančios, jų valdomos ir eksploatuojamos antžeminės infrastruktūros operatoriai, kurie remia kosminių paslaugų teikimą, išskyrus viešųjų elektroninių ryšių tinklų teikėjus

([1]) 2019 m. birželio 5 d. Europos Parlamento ir Tarybos direktyva (ES) 2019/944 dėl elektros energijos vidaus rinkos bendrųjų taisyklių, kuria iš dalies keičiama Direktyva 2012/27/ES (OL L 158, 2019 6 14, p. 125).
([2]) 2019 m. birželio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/943 dėl elektros energijos vidaus rinkos (OL L 158, 2019 6 14, p. 54).
([3]) 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/2001 dėl skatinimo naudoti atsinaujinančių išteklių energiją (OL L 328, 2018 12 21, p. 82).
([4]) 2009 m. rugsėjo 14 d. Tarybos direktyva 2009/119/EB, kuria valstybės narės įpareigojamos išlaikyti privalomąsias žalios naftos ir (arba) naftos produktų atsargas (OL L 265, 2009 10 9, p. 9).
([5]) 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).
([6]) 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).
([7]) 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).
([8]) 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).
([9]) 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).
([10]) 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).
([11]) 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).
([12]) 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).
([13]) 2014 m. gruodžio 18 d. Komisijos deleguotasis reglamentas (ES) 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).
([14]) 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).
([15]) 2013 m. birželio 26 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 575/2013 dėl prudencinių reikalavimų kredito įstaigoms, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 648/2012 (OL L 176, 2013 6 27, p. 1).
([16]) 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).
([17]) 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).
([18]) 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).

([19]) 2022 m. lapkričio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2371 dėl didelių tarpvalstybinio pobūdžio grėsmių sveikatai, kuriuo panaikinamas Sprendimas Nr. 1082/2013/ES (OL L 314, 2022 12 6, p. 26).
([20]) 2001 m. lapkričio 6 d. Europos Parlamento ir Tarybos direktyva 2001/83/EB dėl Bendrijos kodekso, reglamentuojančio žmonėms skirtus vaistus (OL L 311, 2001 11 28, p. 67).
([21]) 2022 m. sausio 25 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/123 dėl didesnio Europos vaistų agentūros vaidmens pasirengimo vaistų ir medicinos priemonių krizei ir jos valdymo srityje (OL L 20, 2022 1 31, p. 1)
([22]) 2020 m. gruodžio 16 d. Europos Parlamento ir Tarybos direktyva (ES) 2020/2184 dėl žmonėms vartoti skirto vandens kokybės (OL L 435, 2020 12 23, p. 1).
([23]) 1991 m. gegužės 21 d. Tarybos direktyva 91/271/EEB dėl miesto nuotėkų valymo (OL L 135, 1991 5 30, p. 40).

II PRIEDAS

KITI ITIN SVARBŪS SEKTORIAI

Sektorius	Subsektorius	Subjekto rūšis
1. Pašto ir kurjerių paslaugos		Pašto paslaugų teikėjai, kaip apibrėžta Direktyvos 97/67/EB 2 straipsnio 1a punkte, įskaitant kurjerių paslaugų teikėjus
2. Atliekų tvarkymas		Atliekas, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2008/98/EB ([1]) 3 straipsnio 9 punkte, tvarkančios įmonės, išskyrus įmones, kurių pagrindinė ekonominė veikla nėra atliekų tvarkymas
3. Cheminių medžiagų gamyba ir platinimas		Chemines medžiagas gaminančios ir chemines medžiagas ar mišinius platinančios įmonės, kaip nurodyta Europos Parlamento ir Tarybos reglamento (EB) Nr. 1907/2006 ([2]) 3 straipsnio 9 ir 14 punktuose, ir gaminius, kaip apibrėžta to reglamento 3 straipsnio 3 punkte, iš tų medžiagų ar mišinių gaminančios įmonės
4. Maisto gamyba, perdirbimas ir platinimas		Maisto verslo įmonės, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (EB) Nr. 178/2002 ([3]) 3 straipsnio 2 punkte, vykdančios didmeninio platinimo ir pramoninės gamybos bei perdirbimo veiklą
5. Gamyba	a) Medicinos priemonių ir *in vitro* diagnostikos medicinos priemonių gamyba	Medicinos priemones, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2017/745 ([4]) 2 straipsnio 1 punkte, gaminantys subjektai, ir *in vitro* diagnostikos medicinos priemones, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2017/746 ([5]) 2 straipsnio 2 punkte, gaminantys subjektai, išskyrus šios direktyvos I priedo 5 punkto penktoje įtraukoje nurodytas medicinos priemones gaminančius subjektus.
	b) Kompiuterinių, elektroninių ir optinių gaminių gamyba	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 26 skyriuje
	c) Elektros įrangos gamyba	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 27 skyriuje
	d) Niekur kitur nepriskirtų mašinų ir įrangos gamyba	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 28 skyriuje
	e) Motorinių transporto priemonių, priekabų ir puspriekabių gamyba	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 29 skyriuje
	f) Kitos transporto įrangos gamyba	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 30 skyriuje

Sektorius	Subsektorius	Subjekto rūšis
6. Skaitmeninių paslaugų teikėjai		— Elektroninių prekyviečių teikėjai
		— Paieškos sistemų teikėjai
		— Socialinių tinklų paslaugų platformos teikėjai
7. Moksliniai tyrimai		Mokslinių tyrimų organizacijos

([1]) 2008 m. lapkričio 19 d. Europos Parlamento ir Tarybos direktyva 2008/98/EB dėl atliekų ir panaikinanti kai kurias direktyvas (OL L 312, 2008 11 22, p. 3).

([2]) 2006 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1907/2006 dėl cheminių medžiagų registracijos, įvertinimo, autorizacijos ir apribojimų (REACH), įsteigiantis Europos cheminių medžiagų agentūrą, iš dalies keičiantis Direktyvą 1999/45/EB bei panaikinantis Tarybos reglamentą (EEB) Nr. 793/93, Komisijos reglamentą (EB) Nr. 1488/94, Tarybos direktyvą 76/769/EEB ir Komisijos direktyvas 91/155/EEB, 93/67/EEB, 93/105/EB bei 2000/21/EB (OL L 396, 2006 12 30, p. 1).

([3]) 2002 m. sausio 28 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 178/2002, nustatantis maistui skirtų teisės aktų bendruosius principus ir reikalavimus, įsteigiantis Europos maisto saugos tarnybą ir nustatantis su maisto saugos klausimais susijusias procedūras (OL L 31, 2002 2 1, p. 1).

([4]) 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/745 dėl medicinos priemonių, kuriuo iš dalies keičiama Direktyva 2001/83/EB, Reglamentas (EB) Nr. 178/2002 ir Reglamentas (EB) Nr. 1223/2009, ir kuriuo panaikinamos Tarybos direktyvos 90/385/EEB ir 93/42/EEB (OL L 117, 2017 5 5, p. 1).

([5]) 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/746 dėl *in vitro* diagnostikos medicinos priemonių, kuriuo panaikinama Direktyva 98/79/EB ir Komisijos sprendimas 2010/227/ES (OL L 117, 2017 5 5, p. 176).

III PRIEDAS

ATITIKTIES LENTELĖ

Direktyva (ES) 2016/1148	Ši direktyva
1 straipsnio 1 dalis	1 straipsnio 1 dalis
1 straipsnio 2 dalis	1 straipsnio 2 dalis
1 straipsnio 3 dalis	-
1 straipsnio 4 dalis	2 straipsnio 12 dalis
1 straipsnio 5 dalis	2 straipsnio 13 dalis
1 straipsnio 6 dalis	2 straipsnio 6 ir 11 dalys
1 straipsnio 7 dalis	4 straipsnis
2 straipsnis	2 straipsnio 14 dalis
3 straipsnis	5 straipsnis
4 straipsnis	6 straipsnis
5 straipsnis	-
6 straipsnis	-
7 straipsnio 1 dalis	7 straipsnio 1 ir 2 dalys
7 straipsnio 2 dalis	7 straipsnio 4 dalis
7 straipsnio 3 dalis	7 straipsnio 3 dalis
8 straipsnio 1–5 dalys	8 straipsnio 1–5 dalys
8 straipsnio 6 dalis	13 straipsnio 4 dalis
8 straipsnio 7 dalis	8 straipsnio 6 dalis
9 straipsnio 1, 2 ir 3 dalys	10 straipsnio 1, 2 ir 3 dalys
9 straipsnio 4 dalis	10 straipsnio 9 dalis
9 straipsnio 5 dalis	10 straipsnio 10 dalis
10 straipsnio 1, 2 dalys ir 3 dalies pirma pastraipa	13 straipsnio 1, 2 ir 3 dalys
10 straipsnio 3 dalies antra pastraipa	23 straipsnio 9 dalis
11 straipsnio 1 dalis	14 straipsnio 1 ir 2 dalys
11 straipsnio 2 dalis	14 straipsnio 3 dalis
11 straipsnio 3 dalis	14 straipsnio 4 dalies pirmos pastraipos a–q ir s punktai bei 7 dalis
11 straipsnio 4 dalis	14 straipsnio 4 dalies pirmos pastraipos r punktas ir antra pastraipa
11 straipsnio 5 dalis	14 straipsnio 8 dalis
12 straipsnio 1–5 dalys	15 straipsnio 1–5 dalys
13 straipsnis	17 straipsnis
14 straipsnio 1 ir 2 dalys	21 straipsnio 1–4 dalys
14 straipsnio 3 dalis	23 straipsnio 1 dalis
14 straipsnio 4 dalis	23 straipsnio 3 dalis
14 straipsnio 5 dalis	23 straipsnio 5, 6 ir 8 dalys

Direktyva (ES) 2016/1148	Ši direktyva
14 straipsnio 6 dalis	23 straipsnio 7 dalis
14 straipsnio 7 dalis	23 straipsnio 11 dalis
15 straipsnio 1 dalis	31 straipsnio 1 dalis
15 straipsnio 2 dalies pirmos pastraipos a punktas	32 straipsnio 2 dalies e punktas
15 straipsnio 2 dalies pirmos pastraipos b punktas	32 straipsnio 2 dalies g punktas
15 straipsnio 2 dalies antra pastraipa	32 straipsnio 3 dalis
15 straipsnio 3 dalis	32 straipsnio 4 dalies b punktas
15 straipsnio 4 dalis	31 straipsnio 3 dalis
16 straipsnio 1 ir 2 dalys	21 straipsnio 1–4 dalys
16 straipsnio 3 dalis	23 straipsnio 1 dalis
16 straipsnio 4 dalis	23 straipsnio 3 dalis
16 straipsnio 5 dalis	-
16 straipsnio 6 dalis	23 straipsnio 6 dalis
16 straipsnio 7 dalis	23 straipsnio 7 dalis
16 straipsnio 8 ir 9 dalys	21 straipsnio 5 dalis ir 23 straipsnio 11 dalis
16 straipsnio 10 dalis	-
16 straipsnio 11 dalis	2 straipsnio 1, 2 ir 3 dalys
17 straipsnio 1 dalis	33 straipsnio 1 dalis
17 straipsnio 2 dalies a punktas	32 straipsnio 2 dalies e punktas
17 straipsnio 2 dalies b punktas	32 straipsnio 4 dalies b punktas
17 straipsnio 3 dalis	37 straipsnio 1 dalies a ir b punktai
18 straipsnio 1 dalis	26 straipsnio 1 dalies b punktas ir 2 dalis
18 straipsnio 2 dalis	26 straipsnio 3 dalis
18 straipsnio 3 dalis	26 straipsnio 4 dalis
19 straipsnis	25 straipsnis
20 straipsnis	30 straipsnis
21 straipsnis	36 straipsnis
22 straipsnis	39 straipsnis
23 straipsnis	40 straipsnis
24 straipsnis	-
25 straipsnis	41 straipsnis
26 straipsnis	45 straipsnis
27 straipsnis	46 straipsnis
I priedo 1 punktas	11 straipsnio 1 dalis
I priedo 2 punkto a papunkčio i–iv punktai	11 straipsnio 2 dalies a–d punktai

Direktyva (ES) 2016/1148	Ši direktyva
I priedo 2 punkto a papunkčio v punktas	11 straipsnio 2 dalies f punktas
I priedo 2 punkto b papunktis	11 straipsnio 4 dalis
I priedo 2 punkto c papunkčio i ir ii punktai	11 straipsnio 5 dalies a punktas
II priedas	I priedas
III priedo 1 ir 2 punktai	II priedo 6 punktas
III priedo 3 punktas	I priedo 8 punktas