EUROPOS
KOMISIJA

Briuselis, 2020 12 16
COM(2020) 823 final

2020/0359 (COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA

dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148

(Tekstas svarbus EEE)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

AIŠKINAMASIS MEMORANDUMAS

1. PASIŪLYMO APLINKYBĖS

• Pasiūlymo pagrindimas ir tikslai

Šis pasiūlymas įtrauktas į rinkinį priemonių, kuriomis siekiama toliau gerinti viešųjų ir privačiųjų subjektų, kompetentingų institucijų ir visos Sąjungos atsparumą ir reagavimą į incidentus kibernetinio saugumo ir ypatingos svarbos infrastruktūros objektų apsaugos srityje. Jis atitinka Komisijos prioritetus užtikrinti, kad Europa prisitaikytų prie skaitmeninio amžiaus, ir kurti perspektyvią žmonėms tarnaujančią ekonomiką. Kibernetinis saugumas yra Komisijos atsako į COVID-19 krizę prioritetas. Rinkiniui priklauso nauja kibernetinio saugumo strategija, kuria siekiama stiprinti Sąjungos strateginę autonomiją ir taip pagerinti jos atsparumą bei kolektyvinį atsaką, taip pat kurti atvirą ir pasaulinį internetą. Galiausiai rinkinyje pateikiamas pasiūlymas dėl direktyvos dėl ypatingos svarbos esminių paslaugų operatorių atsparumo, kuriuo siekiama sumažinti tokiems operatoriams kylančias fizines grėsmes.

Šis pasiūlymas grindžiamas Direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (TIS direktyva) ir ją panaikina. TIS direktyva – tai pirmasis ES lygmens kibernetinio saugumo srities teisės aktas, kuriame nustatytos priemonės, skirtos bendram kibernetinio saugumo lygiui Sąjungoje didinti. TIS direktyva 1) padėjo didinti kibernetinio saugumo pajėgumus nacionaliniu lygmeniu reikalaujant, kad valstybės narės priimtų nacionalines kibernetinio saugumo strategijas ir paskirtų kibernetinio saugumo institucijas; 2) prisidėjo prie glaudesnio valstybių narių bendradarbiavimo Sąjungos lygmeniu sukuriant įvairius forumus, palengvinančius keitimąsi strategine ir operatyvine informacija, ir 3) padidino viešųjų ir privačiųjų subjektų kibernetinį atsparumą septyniuose konkrečiuose sektoriuose (energetikos, transporto, bankų, finansų rinkų infrastruktūros, sveikatos priežiūros, geriamojo vandens tiekimo ir paskirstymo ir skaitmeninės infrastruktūros) ir trijų skaitmeninių paslaugų srityje (elektroninių prekyviečių, paieškos sistemų ir debesijos kompiuterijos paslaugų) reikalaujant, kad valstybės narės užtikrintų, jog esminių paslaugų operatoriai ir skaitmeninių paslaugų teikėjai nustatytų kibernetinio saugumo reikalavimus ir praneštų apie incidentus.

Pasiūlymu atnaujinama dabartinė teisinė sistema atsižvelgiant į didesnį vidaus rinkos skaitmeninimą pastaraisiais metais ir kintančią grėsmių kibernetiniam saugumui padėtį. Abu aspektai dar labiau išryškėjo nuo COVID-19 krizės pradžios. Pasiūlymu taip pat šalinami tam tikri trūkumai, dėl kurių nebuvo galima išnaudoti viso TIS direktyvos potencialo.

Nepaisant reikšmingų laimėjimų, paaiškėjo, kad TIS direktyva, kuri sudarė sąlygas gerokai pakeisti mąstyseną, remiantis instituciniu ir reguliavimo požiūriu į kibernetinį saugumą daugumoje valstybių narių, turi trūkumų. Vykstant skaitmeninei visuomenės transformacijai (kurią dar labiau paskatino COVID-19 krizė), padidėjo grėsmių įvairovė ir atsirado naujų problemų, kurioms spręsti reikalingos pritaikytos ir novatoriškos reagavimo priemonės. Kibernetinių išpuolių toliau daugėja, o įvairūs ES vidaus ir užsienio subjektai vykdo vis sudėtingesnius kibernetinius išpuolius.

TIS direktyvos taikymo vertinimo, kuris buvo atliekamas rengiant poveikio vertinimą, metu nustatytos šios problemos: 1) žemas ES veikiančių įmonių kibernetinio atsparumo lygis; 2) nevienodas atsparumas valstybėse narėse ir sektoriuose ir 3) žemas bendro informuotumo apie padėtį lygis, taip pat bendro reagavimo į krizę nebuvimas. Pavyzdžiui, TIS direktyva netaikoma tam tikros didžiausioms valstybių narių ligoninėms, todėl jos neprivalo įgyvendinti atitinkamų saugumo priemonių, o kitoje valstybėje narėje TIS saugumo reikalavimai taikomi beveik kiekvienam šalies sveikatos priežiūros paslaugų teikėjui.

Pasiūlymu, kuris yra pagal Reglamentavimo kokybės programą (REFIT) įgyvendinama iniciatyva, siekiama sumažinti kompetentingoms institucijoms tenkančią reguliavimo naštą ir viešųjų bei privačiųjų subjektų patiriamas atitikties išlaidas. Visų pirma šio tikslo galima pasiekti panaikinant kompetentingų institucijų pareigą nustatyti esminių paslaugų operatorius ir padidinant saugumo ir pranešimo reikalavimų suderinimo lygį, kad tarpvalstybines paslaugas teikiantiems subjektams būtų lengviau laikytis reguliavimo reikalavimų. Kartu kompetentingoms institucijoms taip pat bus pavestos įvairios naujos užduotys, įskaitant subjektų, veikiančių sektoriuose, kuriems TIS direktyva iki šiol nebuvo taikoma, priežiūrą.

- **Suderinamumas su toje pačioje politikos srityje galiojančiomis nuostatomis**

Šis pasiūlymas priklauso platesniam galiojančių teisinių priemonių rinkiniui ir būsimoms Sąjungos lygmens iniciatyvoms, kuriomis siekiama didinti viešųjų ir privačiųjų subjektų atsparumą grėsmėms.

Kibernetinio saugumo srityje visų pirma Direktyva (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas (kurios kibernetinį saugumą reglamentuojančias nuostatas pakeis šio pasiūlymo nuostatos), ir Pasiūlymas dėl Reglamento dėl skaitmeninės veiklos atsparumo finansų sektoriuje (COM(2020) 595 *final*), įsigaliojus abiem šiems aktams, bus laikomi pasiūlymo *lex specialis.*

Fizinio saugumo srityje pasiūlymas papildo Pasiūlymą dėl direktyvos dėl ypatingos svarbos subjektų atsparumo, kuriuo peržiūrima Direktyva 2008/114/EB dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo (ESI direktyva), kuria Sąjungos lygmeniu sukuriamas Europos ypatingos svarbos infrastruktūros objektų nustatymo procesas bei išdėstomas požiūris į tai, kaip gerinti tokių objektų apsaugą. 2020 m. liepos mėn. Komisija priėmė ES saugumo sąjungos strategiją[1], kurioje pripažino didėjantį fizinės ir skaitmeninės infrastruktūros objektų tarpusavio junglumą ir priklausomybę. Strategijoje pažymėta, kad reikalingas išsamesnis ir nuoseklesnis požiūris į ESI direktyvą ir Direktyvą (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti.

Todėl pasiūlymas iš esmės yra suderintas su Pasiūlymu dėl direktyvos dėl ypatingos svarbos subjektų atsparumo, kuriuo siekiama didinti daugybės sektorių ypatingos svarbos subjektų atsparumą fizinėms grėsmėms. Pasiūlymu siekiama užtikrinti, kad kompetentingos institucijos pagal abu teisės aktus imtųsi papildomų priemonių ir prireikus keistųsi informacija, susijusia su kibernetiniu ir nekibernetiniu atsparumu, ir kad šių sektorių ypatingos svarbos operatoriai, kurie pagal šį pasiūlymą laikomi „esminiais“, taip pat būtų įpareigoti laikytis bendresnio pobūdžio atsparumą didinančių įpareigojimų visų pirma atsižvelgiant į nekibernetinę riziką.

- **Suderinamumas su kitomis Sąjungos politikos sritimis**

Komunikate „Europos skaitmeninės ateities formavimas“[2] pažymima, kad Europai labai svarbu pasinaudoti visais skaitmeninio amžiaus privalumais ir sustiprinti savo pramonės bei inovacijų pajėgumą neperžengiant saugumo ir etikos ribų. Europos duomenų strategijoje nustatyti keturi ramsčiai – duomenų apsauga, pagrindinės teisės, sauga ir kibernetinis saugumas – yra būtinos sąlygos duomenų teikiamomis galimybėmis besinaudojančiai visuomenei.

[1] COM(2020) 605 *final*.
[2] COM(2020) 67 *final*.

2019 m. kovo 12 d. rezoliucijoje Europos Parlamentas paragino *„<..> Komisiją įvertinti poreikį toliau plėsti TIS direktyvos taikymo sritį, į ją įtraukiant kitus svarbius sektorius bei paslaugas, nepatenkančius į konkretiems sektoriams skirtų teisės aktų taikymo sritį“*[3]. Taryba savo 2020 m. birželio 9 d. išvadose palankiai įvertino *„<...> Komisijos planus užtikrinti nuoseklias taisykles rinkos dalyviams ir sudaryti palankesnes sąlygas saugiai, patikimai ir tinkamai dalytis informacija apie grėsmes ir incidentus, be kita ko, peržiūrint Direktyvą dėl tinklų ir informacinių sistemų saugumo (TIS direktyvą), kad būtų ieškoma galimybių padidinti kibernetinį atsparumą ir veiksmingiau reaguoti į kibernetinius išpuolius, ypač į išpuolius prieš esminę ekonominę ir visuomeninę veiklą, kartu atsižvelgiant į valstybių narių kompetenciją, įskaitant atsakomybę už jų nacionalinį saugumą“*.[4] Be to, pasiūlytas teisės aktas nedaro poveikio Sutartyje dėl Europos Sąjungos veikimo (SESV) nustatytų konkurencijos taisyklių taikymui.

Atsižvelgiant į tai, kad didelė dalis kibernetinio saugumo grėsmių kyla už ES ribų, reikalingas nuoseklus požiūris į tarptautinį bendradarbiavimą. Ši direktyva yra pavyzdinis modelis, kurį reikia skatinti ES bendradarbiaujant su trečiosiomis šalimis, visų pirma teikiant išorės techninę pagalbą.

2. TEISINIS PAGRINDAS, SUBSIDIARUMO IR PROPORCINGUMO PRINCIPAI

• Teisinis pagrindas

TIS direktyvos teisinis pagrindas yra Sutarties dėl Europos Sąjungos veikimo 114 straipsnis, kurio tikslas – tobulinant nacionalinių taisyklių suderinimo priemones sukurti veikiančią vidaus rinką. ES Teisingumo Teismas savo sprendime *Vodafone ir kt.* (byla C-58/08) nusprendė, kad nuoroda į SESV 114 straipsnį yra pagrįsta, jeigu nacionalinių taisyklių skirtumai daro tiesioginį poveikį vidaus rinkos veikimui. Teisingumo Teismas taip pat nusprendė, kad tais atvejais, kai SESV 114 straipsniu pagrįstu aktu jau panaikintos visos prekybos kliūtys jo suderintoje srityje, nepanaikinama Sąjungos teisės aktų leidėjo galimybė pritaikyti šį aktą, kad būtų atsižvelgta į pasikeitusias aplinkybes arba žinių raidą, atsižvelgiant į jam tenkančią pareigą užtikrinti Sutartimi pripažintus bendruosius interesus. Galiausiai Teisingumo Teismas nusprendė, kad suderinimo priemonėmis, kurioms taikomas SESV 114 straipsnis, norima suteikti tam tikrą diskreciją priimant sprendimą dėl tinkamiausio metodo, reikalingo pageidaujamam tikslui pasiekti. Ši diskrecija priklausytų nuo klausimo, dėl kurio reikia imtis suderinimo veiksmų, bendro konteksto ir konkrečių aplinkybių. Siūlomu teisės aktu būtų pašalintos kliūtys ir pagerintos galimybės sukurti veikiančią esminių ir svarbių subjektų vidaus rinką, sukuriant aiškias visuotinai taikomas taisykles dėl TIS direktyvos taikymo srities, suderinant taisykles, taikomas kibernetinio saugumo rizikos valdymo ir pranešimo apie incidentus srityje. Dabartiniai skirtumai šioje srityje tiek teisės aktų, tiek priežiūros lygmenimis, taip pat nacionaliniu ir ES lygmenimis trukdo veikti vidaus rinkai, nes tarpvalstybinę veiklą vykdantys subjektai susiduria su skirtingais ir iš dalies sutampančiais reguliavimo reikalavimais ir (arba) jų taikymu pakenkiant galimybei naudotis įsisteigimo laisve ir paslaugų teikimo laisve. Skirtingos taisyklės taip pat turi neigiamą poveikį konkurencijos vidaus rinkoje sąlygoms, kai kalbama apie tos pačios rūšies subjektus įvairiose valstybėse narėse.

[3] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_LT.html.
[4] https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/lt/pdf.

- **Subsidiarumo principas (neišimtinės kompetencijos atveju)**

Kibernetinis atsparumas Sąjungoje negali būti veiksmingas, jeigu bus laikomasi nevienodo nacionaliniu ar regioniniu lygmeniu izoliuoto požiūrio. TIS direktyva šis trūkumas iš dalies buvo išspręstas nacionaliniu ir Sąjungos lygmenimis nustatant tinklų ir informacinių sistemų saugumo sistemą. Tačiau ją perkeliant į nacionalinę tiesę ir įgyvendinant taip pat išryškėjo tam tikrų nuostatų ar požiūrių trūkumai ir ribos, pavyzdžiui, neaiškios direktyvos taikymo srities ribos, dėl kurių atsirado didelių skirtumų, susijusių su *de facto* ES intervencijos mastu ir išsamumu valstybės narės lygmeniu. Be to, nuo COVID-19 krizės pradžios Europos ekonomika kaip niekad anksčiau tapo dar labiau priklausoma nuo tinklų ir informacinių sistemų, o sektoriai ir paslaugos tarpusavyje vis labiau sujungiami. ES intervencija, apimanti daugiau nei dabartines TIS direktyvos priemones, iš esmės yra pateisinama dėl: i) didėjančio su TIS susijusių grėsmių ir problemų tarpvalstybinio pobūdžio; ii) Sąjungos veiksmų siekiant pagerinti ir palengvinti veiksmingą ir koordinuotą nacionalinę politiką potencialo ir iii) suderintų ir bendradarbiavimu grindžiamų politikos priemonių indėlio veiksmingai užtikrinant duomenų apsaugą ir privatumą.

- **Proporcingumo principas**

Šioje direktyvoje siūlomos taisyklės neviršija to, kas yra būtina tam, kad būtų patenkinamai pasiekti konkretūs tikslai. Numatomas saugumo priemonių ir pareigų pranešti suderinimas ir supaprastinimas yra susiję su valstybių narių ir įmonių prašymais tobulinti dabartinę sistemą.

Pasiūlyme atsižvelgiama į valstybėse narėse jau galiojančią praktiką. Dėl tokių supaprastintų ir koordinuotų reikalavimų pasiektas didesnis apsaugos lygis yra proporcingas didėjančiai rizikai, su kuria susiduriama, įskaitant tarpvalstybinį aspektą turinčią riziką; jie pagrįstai ir visuotinai atitinka subjektų, dalyvaujančių užtikrinant savo teikiamų paslaugų tęstinumą ir kokybę, interesą. Sisteminio valstybių narių bendradarbiavimo užtikrinimo išlaidos turėtų būti nedidelės, palyginti su ekonominiais ir visuomeniniais nuostoliais bei žala, kurią sukelia kibernetinio saugumo incidentai. Be to, iš konsultacijų su suinteresuotosiomis šalimis, kurios buvo surengtos peržiūrint TIS direktyvą, įskaitant atvirų viešų konsultacijų ir tikslinių apklausų rezultatus, matyti, kad TIS direktyvos peržiūrai, atsižvelgiant į minėtas nuostatas, pritariama.

- **Priemonės pasirinkimas**

Pasiūlymu bus dar labiau supaprastintos įmonėms nustatytos pareigos ir užtikrinamas aukštesnio lygio šių pareigų suderinimas. Kartu pasiūlymu siekiama suteikti valstybėms narėms reikalingą lankstumą, kad jos galėtų atsižvelgti į nacionalinius ypatumus (pvz., galimybė nustatyti papildomus esminius arba svarbius subjektus, kurie nenumatyti teisės akte). Todėl būsima teisinė priemonė turėtų būti direktyva, nes ši teisinė priemonė sudaro sąlygas imtis tikslingų didesnio suderinimo veiksmų ir suteikia tam tikrą lankstumą kompetentingoms institucijoms.

3. *EX POST* VERTINIMO, KONSULTACIJŲ SU SUINTERESUOTOSIOMIS ŠALIMIS IR POVEIKIO VERTINIMO REZULTATAI

- **Galiojančių teisės aktų *ex post* vertinimas / tinkamumo patikrinimas**

Komisija atliko TIS direktyvos taikymo vertinimą[5]. Ji išanalizavo jos aktualumą, Europos pridėtinę vertę, nuoseklumą, veiksmingumą ir efektyvumą. Pagrindinės šios analizės išvados yra šios:

- TIS direktyvos taikymo sritis yra pernelyg ribota atsižvelgiant į sektorius, kuriems ji taikoma, ir taip iš esmės yra dėl: i) padidėjusio skaitmeninimo pastaraisiais metais ir didesnio tarpusavio junglumo, ii) to, kad TIS direktyvos taikymo sritis nebeatspindi visų skaitmenintų sektorių, kuriuose teikiamos pagrindinės paslaugos ekonomikai ir visai visuomenei.
- TIS direktyva nėra pakankamai aiški, kai kalbama apie jos taikymo sritį esminių paslaugų operatoriams, be to, jos nuostatose nėra pakankamai paaiškinama nacionalinė kompetencija skaitmeninių paslaugų teikėjų atžvilgiu. Dėl šios priežasties susidarė situacija, kurioje tam tikrų rūšių subjektai nebuvo nustatyti visose valstybėse narėse, todėl jie neprivalo nustatyti saugumo priemonių ir pranešti apie incidentus.
- TIS direktyva valstybėms narėms suteikta plati diskrecija nustatyti esminių paslaugų operatoriams taikomus saugumo ir pranešimo apie incidentus reikalavimus. Iš vertinimo matyti, kad kai kuriais atvejais valstybės narės šiuos reikalavimus įgyvendino labai nevienodai, todėl daugiau nei vienoje valstybėje narėje veikiančioms įmonėms buvo užkrauta papildoma našta.
- TIS direktyvos priežiūros ir vykdymo užtikrinimo režimas yra neveiksmingas. Pavyzdžiui, valstybės narės labai nenoriai skyrė baudas subjektams, kurie nesilaikė saugumo reikalavimų arba nepranešė apie incidentus. Tai gali turėti neigiamų pasekmių pavienių subjektų kibernetiniam atsparumui.
- Finansiniai ir žmogiškieji ištekliai, kuriuos valstybės narės skiria tam, kad įvykdytų savo užduotis (pvz., esminių paslaugų operatorių nustatymas arba priežiūra), taigi ir nevienodas brandos lygis sprendžiant su kibernetinio saugumo rizika susijusius klausimus, yra labai skirtingi. Dėl šios priežasties dar labiau padidėja valstybių narių kibernetinio atsparumo skirtumai.
- Valstybės narės sistemiškai nesidalija informacija viena su kita, todėl atsiranda neigiamų pasekmių visų pirma kibernetinio saugumo priemonių veiksmingumui ir bendro informuotumo apie padėtį ES lygmeniu lygiui. Tą patį galima pasakyti apie dalijimąsi informacija tarp privačių subjektų ir ES bendradarbiavimo struktūrų ir privačiųjų subjektų dalyvavimą.

- **Konsultacijos su suinteresuotosiomis šalimis**

Komisija konsultavosi su įvairiomis suinteresuotosiomis šalimis. Valstybių narių ir suinteresuotųjų šalių buvo prašoma dalyvauti atvirose viešose konsultacijose ir apklausose bei praktiniuose seminaruose, kuriuos Komisijos prašymu surengė bendrovė „Wavestone“, CEPS ir ICF, kad atliktų tyrimą, kuriuo remiantis būtų peržiūrima TIS direktyva. Suinteresuotosioms šalims, su kuriomis buvo konsultuojamasi, priklausė kompetentingos institucijos, Sąjungos įstaigos, sprendžiančios su kibernetiniu saugumu susijusius klausimus,

[5] [Poveikio vertinimo 5 priedas]

esminių paslaugų operatoriai, skaitmeninių paslaugų teikėjai, subjektai, teikiantys paslaugas, kurioms netaikoma dabartinė TIS direktyva, verslo asociacijos ir vartotojų organizacijos bei piliečiai.

Be to, Komisija nuolat palaikė ryšį su kompetentingomis institucijomis, atsakingomis už TIS direktyvos įgyvendinimą. Bendradarbiavimo grupė išsamiai aptarė įvairius kompleksinius ir sektorinius įgyvendinimo aspektus. Galiausiai per savo TIS šalių vizitus 2019 ir 2020 m. Komisija apklausė 154 viešuosius ir privačiuosius subjektus, taip pat 117 kompetentingų institucijų.

- **Tiriamųjų duomenų rinkimas ir naudojimas**

Komisija pasamdė bendrovės „Wavestone“, CEPS ir ICF konsorciumą, kad jis padėtų jai peržiūrėti TIS direktyvą[6]. Rangovas, rengdamas tikslines apklausas ir praktinius seminarus, susisiekė ne tik su suinteresuotosiomis šalimis, kurioms TIS direktyva daro tiesioginį poveikį, bet ir konsultavosi su įvairiais kibernetinio saugumo srities ekspertais, pavyzdžiui, kibernetinio saugumo tyrėjais ir kibernetinio saugumo pramonės specialistais.

- **Poveikio vertinimas**

Prie šio pasiūlymo pridedamas poveikio vertinimas[7], kuris Reglamentavimo patikros valdybai buvo pateiktas 2020 m. spalio 23 d., o teigiama nuomonė su Reglamentavimo patikros valdybos pastabomis gauta 2020 m. lapkričio 20 d. Reglamentavimo patikros valdyba rekomendavo pasiūlymą tam tikrose srityse patobulinti siekiant: 1) analizuojant problemas geriau aptarti tarpvalstybinio šalutinio poveikio svarbą; 2) geriau paaiškinti, kada iniciatyva būtų laikoma sėkmingai įgyvendinta; 3) papildomai pagrįsti politikos galimybių sąrašą; 4) išsamiau aptarti siūlomų priemonių išlaidas. Poveikio vertinimas buvo patikslintas, kad būtų atsižvelgta į šiuos aspektus, taip pat į išsamesnes Reglamentavimo patikros valdybos pastabas. Dabar jame pateikiami išsamesni paaiškinimai dėl tarpvalstybinio šalutinio poveikio kibernetinio saugumo srityje, aiškesnė sėkmės įvertinimo apžvalga, išsamesnis įvairių politikos galimybių ir veiksmų, kurių svarstoma imtis pagal šias politikos galimybes, struktūros ir logikos paaiškinimas, išsamesnis aspektų, kurie analizuojami atsižvelgiant į TIS direktyvos taikymo sritį sektoriams, paaiškinimas ir papildomi paaiškinimai dėl išlaidų.

Komisija išnagrinėjo įvairias politikos galimybes, kuriomis siekiama patobulinti teisinę sistemą kibernetinio atsparumo ir reagavimo į incidentus srityje:

- „nieko nekeisti“: TIS direktyva liktų nepakitusi ir nebūtų imtasi jokių kitų neteisinio pobūdžio priemonių siekiant išspręsti TIS direktyvos vertinimo metu nustatytas problemas;
- 1 galimybė: teisėkūros lygmeniu nebūtų atliekami jokie pakeitimai. Vietoj to, Komisija, pasikonsultavusi su Bendradarbiavimo grupe, ES kibernetinio saugumo agentūra (ENISA) ir, kai taikytina, reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) tinklu, priimtų rekomendacijas ir gaires (pvz., dėl esminių paslaugų operatorių nustatymo, saugumo reikalavimų, pranešimo apie incidentus procedūrų ir priežiūros);

[6] Tyrimas, kuriuo siekiama prisidėti prie Direktyvos (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (TIS direktyva) peržiūros, Nr. 2020-665. Bendrovė „Wavestone“, CEPS ir ICF.

[7] **[Turi būti pridėtos nuorodos į galutinį dokumentą ir santrauką.]**

- 2 galimybė: ši galimybė apima tikslingus TIS direktyvos pakeitimus, įskaitant taikymo srities praplėtimą ir keletą kitų pakeitimų, kuriais būtų siekiama garantuoti tam tikrus skubius nustatytų problemų sprendimus, šiuo tikslu suteikiant daugiau aiškumo ir užtikrinant tolesnį suderinimą (pvz., nuostatos, kuriomis suderinamos nustatymo ribos). Tačiau iš dalies pakeistoje TIS direktyvoje išliktų pagrindinės sudedamosios dalys, požiūris ir loginis pagrindas;
- 3 galimybė: pagal šį scenarijų būtų atliekami sisteminiai ir struktūriniai TIS direktyvos pakeitimai (priimant naują direktyvą), kuriais būtų numatyta pakeisti kai kuriuos esminius požiūrio aspektus siekiant atsižvelgti į platesnį visos Sąjungos ekonomikos segmentą kartu daugiau dėmesio skiriant didelių ir pagrindinių dalyvių priežiūrai. Pagal šį scenarijų taip pat būtų supaprastintos įmonėms nustatytos pareigos ir užtikrinamas aukštesnis tokių pareigų suderinimo lygis, sukuriama veiksmingesnė aplinka, susijusi su veiklos aspektais, taip pat nustatomas aiškus įvairių suinteresuotųjų šalių bendrų pareigų ir atskaitomybės pagrindas.

Poveikio vertinime daroma išvada, kad tinkamiausia yra 3 galimybė (t. y. sisteminiai ir struktūriniai TIS sistemos pakeitimai). Kalbant apie veiksmingumą pažymėtina, kad pagal tinkamiausią galimybę būtų aiškiai nustatoma TIS direktyvos taikymo sritis, kuri būtų praplėsta taip, kad apimtų reprezentatyvesnę ES ekonomikos sektorių ir visuomenės grupių dalį, be to, būtų supaprastinami reikalavimai, įskaitant griežčiau apibrėžtą priežiūros ir vykdymo užtikrinimo sistemą, kuria būtų siekiama padidinti atitikties lygį. Joje taip pat numatytos priemonės, kurių paskirtis – patobulinti požiūrį į politikos formavimą valstybių narių lygmeniu ir pakeisti tokių požiūrių paradigmą, skatinti naujas tiekėjų santykių rizikos valdymo sistemas ir suderintą pažeidžiamumų atskleidimą. Kartu pagal tinkamiausią politikos galimybę nustatomas aiškus bendrų pareigų ir atskaitomybės pagrindas ir numatomi mechanizmai, kuriais siekiama skatinti didesnį valstybių narių, taip pat institucijų ir pramonės tarpusavio pasitikėjimą, skatinamas dalijimasis informacija ir užtikrinamas labiau operatyvinis požiūris, pavyzdžiui, savitarpio pagalbos ir tarpusavio vertinimo mechanizmai. Pagal šią galimybę taip pat būtų numatyta ES krizių valdymo sistema, grindžiama neseniai pradėjusiu veikti ES operaciniu tinklu, taip pat būtų užtikrintas aktyvesnis ENISA dalyvavimas, atsižvelgiant į jos dabartinius įgaliojimus, užtikrinant tikslų supratimą apie kibernetinio saugumo padėtį Sąjungoje.

Kalbant apie veiksmingumą pažymėtina, kad nors dėl tinkamiausios galimybės įmonės ir valstybės narės patirtų papildomų atitikties ir vykdymo užtikrinimo išlaidų, ja taip pat būtų prisidedama prie abipusės naudos ir sinergijos, be to, tinkamiausia galimybė iš visų analizuotų politikos galimybių turi didžiausią potencialą užtikrinti didesnį ir nuoseklesnį pagrindinių subjektų visoje Sąjungoje kibernetinio atsparumo lygį, kuris galiausiai padėtų įmonėms ir visuomenei sutaupyti sąnaudų. Dėl šios politikos galimybės valstybių narių valdžios institucijos susidurtų su papildoma administracine našta ir patirtų atitikties išlaidų. Tačiau, atsižvelgus į viską, vidutinės ir ilgalaikės trukmės laikotarpiu dėl glaudesnio valstybių narių bendradarbiavimo taip pat būtų gauta esminės naudos, įskaitant naudą veiklos lygmeniu, be to, užtikrinant savitarpio pagalbą būtų skatinami tarpusavio vertinimo mechanizmai ir geresnis pagrindinių įmonių bendras supratimas ir sąveika su jomis, ir apskritai padidėtų kibernetinio saugumo pajėgumai nacionaliniu ir regioniniu lygmenimis. Tinkamiausia politikos galimybė taip pat padėtų užtikrinti didesnio masto suderinamumą su kitais teisės taktais, iniciatyvomis arba politikos priemonėmis, įskaitant konkrečių sektorių *lex specialis*.

Sprendžiant dabartinę sisteminę nepakankamos kibernetinio saugumo parengties problemą, kuri egzistuoja valstybių narių ir įmonių bei kitų organizacijų lygmeniu, gali būti padidintas efektyvumas ir sumažintos papildomos išlaidos, atsirandančios dėl kibernetinio saugumo incidentų.

- Dėl didesnio kibernetinio saugumo parengties lygio esminiai ir svarbūs subjektai galėtų sumažinti galimus nuostolius, kuriuos sukelia sutrikimai, įskaitant pramoninį šnipinėjimą, ir dideles išlaidas, reikalingas *ad hoc* grėsmių mažinimui. Tikėtina, kad tokia nauda bus didesnė nei būtinos investicinės išlaidos. Sumažinus vidaus rinkos susiskaidymą, taip pat pagerėtų operatorių veikimo sąlygos.
- Valstybių narių atveju tai padėtų dar labiau sumažinti *ad hoc* grėsmių švelninimui skirtų biudžeto išlaidų didėjimo riziką ir papildomų išlaidų, patiriamų susidarius ekstremaliajai situacijai dėl kibernetinio saugumo incidentų, riziką.
- Tikėtina, kad kibernetinio saugumo incidentų šalinimas sumažins piliečių pajamų nuostolius, kurie atsiranda dėl ekonomikos sutrikimo.

Labai tikėtina, kad dėl padidėjusio kibernetinio saugumo lygio valstybėse narėse ir įmonių bei institucijų gebėjimo greitai reaguoti į incidentą ir sumažinti jo poveikį padidės bendras piliečių pasitikėjimas skaitmenine ekonomika, o tai galėtų turėti teigiamą poveikį augimui ir investicijoms.

Tikėtina, kad dėl didėjančio bendro kibernetinio saugumo lygio padidės bendras saugumas ir sklandžiai bei nepertraukiamai bus teikiamos esminės paslaugos, kurios yra ypač svarbios visuomenei. Iniciatyva taip pat gali turėti kitų socialinių pasekmių, pavyzdžiui, mažesnis kibernetinių nusikaltimų ir terorizmo lygis ir geresnė civilinė sauga. Didėjantis įmonių ir kitų organizacijų kibernetinės parengties lygis gali padėti išvengti galimų finansinių nuostolių, patiriamų dėl kibernetinių išpuolių, taip užkertant kelią poreikiui atleisti darbuotojus.

Didėjantis bendras kibernetinio saugumo lygis taip pat galėtų užkirsti kelią rizikai ir (arba) žalai aplinkai, jei būtų surengtas išpuolis prieš esminę paslaugą. Tai būtų galima pasakyti visų pirma apie energetikos, vandens tiekimo ir paskirstymo arba transporto sektorius. Iniciatyva sustiprinus kibernetinio saugumo pajėgumus būtų galima dažniau naudoti naujausios kartos IRT infrastruktūros objektus ir paslaugas, kurios yra tvaresnės ir aplinkosaugos požiūriu, ir pakeisti neveiksmingus ir ne tokius saugius senus infrastruktūros objektus. Tikimasi, kad tai taip pat padės sumažinti brangių kibernetinių incidentų skaičių ir atlaisvinti tvarioms investicijoms prieinamas lėšas.

- **Reglamentavimo tinkamumas ir supaprastinimas**

Pasiūlyme numatyta TIS taikymo bendroji išimtis labai mažiems ir mažiesiems subjektams ir švelnesnis *ex post* priežiūros režimas, taikomas daugumai naujų subjektų atsižvelgiant į peržiūrėtą taikymo sritį (vadinamieji svarbūs subjektai). Šiomis priemonėmis siekiama kuo labiau sumažinti įmonėms ir viešojo administravimo institucijoms tenkančią naštą ir išlaikyti tokios naštos pusiausvyrą. Be to, pasiūlymu sudėtinga esminių paslaugų operatorių nustatymo sistema pakeičiama visuotinai taikoma pareiga, be to, nustatomas aukštesnis saugumo ir pareigų pranešti suderinimo lygis, kuris turėtų padėti sumažinti atitikties naštą, ypač tarpvalstybines paslaugas teikiantiems subjektams.

Pasiūlymu kuo labiau sumažinamos MVĮ patiriamos atitikties išlaidos, nes subjektai privalo imtis tik tų priemonių, kurios yra būtinos užtikrinti tokį tinklų ir informacinių sistemų saugumo lygį, kuris atitinka kylančią riziką.

- **Pagrindinės teisės**

ES yra įsipareigojusi užtikrinti, kad būtų laikomasi pagrindinių teisių apsaugos aukštų standartų. Visos subjektų savanoriško dalijimosi informacija sistemos, kuriomis naudotis skatinama šia direktyva, būtų įgyvendinamos patikimoje aplinkoje visapusiškai laikantis

Sąjungos duomenų apsaugos taisyklių, visų pirma Europos Parlamento ir Tarybos reglamento (ES) 2016/679[8].

4. POVEIKIS BIUDŽETUI

Žr. finansinę pažymą.

5. KITI ELEMENTAI

- **Įgyvendinimo planai ir stebėsena, vertinimas ir ataskaitų teikimo tvarka**

Į pasiūlymą įtrauktas bendras poveikio konkretiems tikslams stebėsenos ir vertinimo planas, pagal kurį Komisija praėjus ne daugiau kaip [54 mėnesiams] nuo įsigaliojimo datos privalo atlikti peržiūrą ir pateikti pagrindinių išvadų ataskaitą Europos Parlamentui ir Tarybai.

Peržiūra turi būti atliekama vadovaujantis Komisijos geresnio reglamentavimo gairėmis.

- **Išsamus konkrečių pasiūlymo nuostatų paaiškinimas**

Pasiūlymo struktūra grindžiama keliomis pagrindinėmis tarpusavyje susijusiomis politikos sritimis, kurios padeda didinti kibernetinio saugumo lygį Sąjungoje.

Dalykas ir taikymo sritis (1 ir 2 straipsniai)

Direktyva visų pirma: a) nustatomos valstybių narių pareigos priimti nacionalinę kibernetinio saugumo strategiją, paskirti kompetentingas nacionalines institucijas, bendruosius informacinius centrus ir CSIRT; b) numatoma, kad valstybės narės nustato kibernetinio saugumo rizikos valdymo pareigas ir pareigas pranešti, taikomas subjektams, kurie I priede įvardijami kaip esminiai subjektai, ir subjektams, kurie II priede įvardijami kaip svarbūs subjektai; c) numatoma, kad valstybės narės nustato pareigas, susijusias su dalijimusi kibernetinio saugumo informacija.

Ji taikoma tam tikriems viešiesiems arba privatiesiems esminiams subjektams, veikiantiems I priede išvardytuose sektoriuose (energetikos; transporto; bankininkystės; finansų rinkų infrastruktūrų; sveikatos, geriamojo vandens; nuotekų; skaitmeninės infrastruktūros; viešojo administravimo ir kosmoso), ir tam tikriems svarbiems subjektams, veikiantiems II priede išvardytuose sektoriuose (pašto ir pasiuntinių paslaugų; atliekų tvarkymo; cheminių medžiagų gamybos ir platinimo; maisto gamybos, perdirbimo ir platinimo; gamybos ir skaitmeninių paslaugų teikimo). Labai maži ir mažieji subjektai, kaip apibrėžta 2003 m. gegužės 6 d. Komisijos rekomendacijoje 2003/361/EB, nepatenka į direktyvos taikymo sritį, išskyrus elektroninių ryšių tinklų paslaugų teikėjus ar viešai prieinamų elektroninių ryšių paslaugų teikėjus, patikimumo užtikrinimo paslaugų teikėjus, aukščiausio lygio domenų (TLD) vardų registrus ir viešojo administravimo ir tam tikrus kitus subjektus, pavyzdžiui, vienintelis paslaugų teikėjas valstybėje narėje.

Nacionalinės kibernetinio saugumo sistemos (5–11 straipsniai)

[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).

Valstybės narės privalo priimti nacionalinę kibernetinio saugumo strategiją, kurioje apibrėžiami strateginiai uždaviniai ir tinkamos politikos bei reguliavimo priemonės, kad būtų pasiektas ir išlaikytas aukšto lygmens kibernetinis saugumas.

Direktyva taip pat nustatoma suderinto pažeidžiamumų atskleidimo sistema ir reikalaujama, kad valstybės narės paskirtų CSIRT, kurios veiktų kaip patikimi tarpininkai ir palengvintų pranešimus teikiančių subjektų ir gamintojų arba IRT produktų ir IRT paslaugų teikėjų sąveiką. ENISA privalo sukurti ir tvarkyti Europos pažeidžiamumų registrą, kuriame registruojami nustatyti pažeidžiamumai.

Valstybės narės privalo nustatyti nacionalines kibernetinio saugumo krizių valdymo sistemas *inter alia* paskirdamos nacionalines kompetentingas institucijas, atsakingas už didelio masto kibernetinio saugumo incidentų ir krizių valdymą.

Valstybės narės taip pat privalo paskirti vieną arba daugiau nacionalinių kompetentingų kibernetinio saugumo institucijų, kurios būtų atsakingos už priežiūros užduočių pagal šią direktyvą vykdymą, ir bendrąjį informacinį centrą kibernetinio saugumo klausimais, kuris vykdytų ryšių palaikymo funkciją ir užtikrintų tarpvalstybinį valstybių narių valdžios institucijų bendradarbiavimą. Valstybės narės taip pat privalo paskirti CSIRT.

Bendradarbiavimas (12–16 straipsniai)

Direktyva sudaroma Bendradarbiavimo grupė, kad būtų remiamas ir lengvinamas valstybių narių strateginis bendradarbiavimas ir keitimasis informacija, taip pat didinama jų atsakomybė ir pasitikėjimas. Ja taip pat sukuriamas CSIRT tinklas, kuriuo siekiama prisidėti prie valstybių narių atsakomybės ir tarpusavio pasitikėjimo didinimo ir skatinamas greitas bei veiksmingas operatyvinis bendradarbiavimas.

Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas („EU-CyCLONe“) sukuriamas siekiant remti koordinuotą didelio masto kibernetinio saugumo incidentų ir krizių valdymą ir užtikrinti nuolatinį keitimąsi informacija tarp valstybių narių ir ES institucijų.

ENISA, bendradarbiaudama su Komisija, kas dvejus metus privalo parengti metinę kibernetinio saugumo būklės Sąjungoje ataskaitą.

Komisija privalo nustatyti tarpusavio vertinimo sistemą, kuri sudarytų sąlygas nuolat atlikti valstybių narių kibernetinio saugumo politikos veiksmingumo tarpusavio vertinimus.

Kibernetinio saugumo rizikos valdymas ir pareigos pranešti (17–23 straipsniai)

Valstybės narės pagal direktyvą privalo numatyti, kad visų subjektų, kuriems taikoma direktyva, valdymo organai tvirtintų kibernetinio saugumo rizikos valdymo priemones, kurių ėmėsi atitinkami subjektai, ir dalyvautų konkrečiuose su kibernetiniu saugumu susijusiuose mokymuose.

Valstybės narės privalo užtikrinti, kad subjektai, kuriems taikoma direktyva, imtųsi tinkamų ir proporcingų techninių ir organizacinių priemonių, kad suvaldytų tinklų ir informacinių sistemų saugumui kylančią kibernetinio saugumo riziką. Jos taip pat privalo užtikrinti, kad subjektai praneštų nacionalinėms kompetentingoms institucijoms arba CSIRT apie bet kokį kibernetinio saugumo incidentą, kuris turi didelį poveikį jų teikiamai paslaugai.

Aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys aukščiausio lygio domenų vardų registracijos paslaugas, renka ir saugo tikslius ir išsamius domeno vardų registracijos duomenis. Be to, tokie subjektai privalo teisėtiems prieigos prašytojams leisti veiksmingai susipažinti su domeno registracijos duomenimis.

Jurisdikcija ir registracija (24 ir 25 straipsniai)

Paprastai laikoma, kad esminiai ir svarbūs subjektai priklauso valstybės narės, kurioje jie teikia paslaugas, jurisdikcijai. Tačiau laikoma, kad tam tikrų rūšių subjektai (DNS paslaugų teikėjai, aukščiausio lygio domenų vardų registrai, debesijos kompiuterijos paslaugų teikėjai, duomenų centrų paslaugų teikėjai ir turinio teikimo tinklo paslaugų tiekėjai, taip pat tam tikri skaitmeninių paslaugų teikėjai) priklauso valstybės narės, kurioje yra jų pagrindinė buveinė Sąjungoje, jurisdikcijai. Taip siekiama užtikrinti, kad tokiems subjektams nebūtų taikomi įvairūs skirtingi teisiniai reikalavimai, nes jie tarpvalstybines paslaugas teikia itin plačiu mastu. ENISA privalo sukurti ir tvarkyti tokios rūšies subjektų registrą.

Dalijimasis informacija (26 ir 27 straipsniai)

Valstybės narės numato taisykles, kuriomis subjektams sudaromos sąlygos dalyvauti dalijantis su kibernetiniu saugumu susijusia informacija laikantis konkrečių dalijimosi kibernetinio saugumo informacija taisyklių sistemos pagal SESV 101 straipsnį. Be to, valstybės narės sudaro sąlygas subjektams, kuriems ši direktyva netaikoma, savanoriškai pranešti apie rimtus incidentus, kibernetines grėsmes arba vos neįvykusius incidentus.

Priežiūra ir vykdymo užtikrinimas (28–34 straipsniai)

Kompetentingos institucijos privalo prižiūrėti subjektus, kuriems taikoma ši direktyva, ir visų pirma užtikrinti, kad jie laikytųsi saugumo ir pranešimo apie incidentus reikalavimų. Joje daromas skirtumas tarp *ex ante* priežiūros režimo, taikomo esminiams subjektams, ir *ex post* priežiūros režimo, taikomo svarbiems subjektams, pastaruoju atveju reikalaujant, kad kompetentingos institucijos imtųsi veiksmų, kai joms pateikiami įrodymai arba matomi požymiai, kad svarbus subjektas nesilaiko saugumo ir pranešimo apie incidentą reikalavimų.

Pagal direktyvą taip pat reikalaujama, kad valstybės narės skirtų administracines baudas esminiams ir svarbiems subjektams ir nustatytų tam tikras didžiausias baudas.

Valstybės narės privalo bendradarbiauti ir prireikus padėti viena kitai, kai subjektai teikia paslaugas daugiau nei vienoje valstybėje narėje arba kai subjekto pagrindinė buveinė arba jo atstovybė yra tam tikroje valstybėje narėje, tačiau jos tinklų ir informacinės sistemos yra vienoje arba keliose kitose valstybėse narėse.

2020/0359 (COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA

dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148

(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 ekonomikos ir socialinių reikalų komiteto nuomonę[9],

atsižvelgdami į Regionų komiteto nuomonę[10],

laikydamiesi įprastos teisėkūros procedūros,

kadangi:

(1) Europos Parlamento ir Tarybos direktyva (ES) 2016/1148[11] 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 kibernetiniams incidentams, ir taip prisidėti prie veiksmingo Sąjungos ekonomikos ir visuomenės veikimo;

(2) nuo Direktyvos (ES) 2016/1148 įsigaliojimo padaryta didelė pažanga didinant Sąjungos kibernetinio atsparumo lygį. Persvarsčius tą direktyvą, paaiškėjo, kad ji tapo institucinio ir reguliavimo požiūrio į kibernetinį saugumą Sąjungoje paskata ir sudarė sąlygas reikšmingam mąstysenos pokyčiui. Ta direktyva padėjo galutinai sukurti nacionalines sistemas apibrėžiant nacionalines kibernetinio saugumo strategijas, nustatant nacionalinius pajėgumus ir įgyvendinant reguliavimo priemones, taikomas kiekvienos valstybės narės nustatytiems esminiams infrastruktūros objektams ir dalyviams. Ja taip pat prisidėta prie bendradarbiavimo Sąjungos lygmeniu šiuo tikslu sudarant Bendradarbiavimo grupę[12] ir sukuriant nacionalinių reagavimo į kompiuterinius saugumo incidentus tarnybų tinklą (CSIRT tinklas)[13]. Nepaisant šių

---

9 OL C , , p. .

10 OL C , , p. .

11 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 194/1, 2016 7 19, p. 1).

12 Direktyvos (ES) 2016/1148 11 straipsnis.

13 Direktyvos (ES) 2016/1148 12 straipsnis.

laimėjimų, peržiūrėjus Direktyvą (ES) 2016/1148 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 grėsmių kibernetiniam saugumui padėtis tapo sudėtingesnė, atsirado naujų problemų, į kurias visos valstybės narės turi reaguoti prisitaikydamos, koordinuotai ir naujoviškai. Kibernetinio saugumo incidentų skaičius, mastas, sudėtingumas, dažnumas ir poveikis didėja ir kelia didelę grėsmę tinklų ir informacinių sistemų veikimui. Todėl kibernetiniai incidentai gali trukdyti vykdyti ekonominę veiklą vidaus rinkoje, sukelti finansinių nuostolių, pakirsti naudotojų pasitikėjimą ir padaryti didelę žalą Sąjungos ekonomikai ir visuomenei. Todėl kibernetinio saugumo parengtis ir veiksmingumas kaip niekad anksčiau yra labai svarbūs tinkamam vidaus rinkos veikimui;

(4) Direktyvos (ES) 1148/2016 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. Paslaugas teikiantiems arba svarbią ekonominę veiklą vykdantiems subjektams nustatyti kibernetinio saugumo reikalavimai valstybėse narės gerokai skiriasi atsižvelgiant į reikalavimo rūšį, jų išsamumo lygį ir priežiūros metodą. Dėl šių skirtumų patiriama papildomų išlaidų, o prekes ar paslaugas tarpvalstybiniu mastu tiekiančioms įmonėms kyla sunkumų. Vienos valstybės narės nustatyti reikalavimai, kurie skiriasi nuo kitos valstybės narės nustatytų reikalavimų arba net jiems prieštarauja, gali daryti didelį neigiamą poveikį šiai tarpvalstybinei veiklai. Be to, tikėtina, kad dėl nepakankamai optimalios kibernetinio saugumo standartų struktūros arba įgyvendinimo vienoje valstybėje narėje kils pasekmių kitų valstybių narių kibernetinio saugumo lygiui, visų pirma atsižvelgiant į intensyvius tarpvalstybinius mainus. Peržiūrėjus Direktyvą (ES) 2016/1148, paaiškėjo, kad valstybėse narėse ji įgyvendinama labai įvairiai, be kita ko, skiriasi jos taikymo sritis, 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 įgyvendinti joje nustatytas saugumo pareigas ir pareigas pranešti apie incidentus. Todėl šios pareigos nacionaliniu lygmeniu buvo įgyvendintos gana skirtingai. Panašūs skirtumai nustatyti direktyvos nuostatų dėl priežiūros ir vykdymo užtikrinimo įgyvendinimo srityje;

(5) visi šie skirtumai lemia vidaus rinkos susiskaidymą ir gali kenkti vidaus rinkos veikimui, visų pirma tai pasakytina apie neigiamą poveikį tarpvalstybiniam paslaugų teikimui ir kibernetinio saugumo atsparumo lygiui, kurį lemia taikomi skirtingi standartai. Šia direktyva siekiama pašalinti tokius didelius skirtumus tarp valstybių narių, visų pirma nustatant būtinas taisykles, susijusias su koordinuotos reguliavimo sistemos veikimu, šiuo tikslu sukuriant kiekvienos valstybės narės atsakingų institucijų veiksmingo bendradarbiavimo mechanizmus, atnaujinant sektorių ir veiklos, kuriems taikomos kibernetinio saugumo pareigos, sąrašą ir numatant veiksmingas teisių gynimo priemones ir sankcijas, kurios yra labai svarbios šių pareigų vykdymui veiksmingai užtikrinti. Todėl Direktyva (ES) 2016/1148 turėtų būti panaikinta ir pakeista šia direktyva;

(6) ši direktyva nedaro poveikio valstybių narių galimybei imtis priemonių, būtinų gyvybiniams jos saugumo interesams užtikrinti, viešajai tvarkai palaikyti bei visuomenės saugumui užtikrinti, ir sudaryti sąlygas tirti bei išsiaiškinti nusikalstamas veikas ir už jas patraukti baudžiamojon atsakomybėn pagal Sąjungos teisę. Pagal SESV 346 straipsnį jokia valstybė narė neturi būti įpareigota teikti informacijos,

kurios atskleidimas, jos nuomone, prieštarautų esminiams jos viešojo saugumo interesams. Šiomis aplinkybėmis svarbios nacionalinės ir Sąjungos taisyklės dėl įslaptintos informacijos apsaugos, susitarimai dėl informacijos neatskleidimo ir neoficialūs susitarimai dėl informacijos neatskleidimo, pavyzdžiui, Srauto kontrolės protokolas[14];

(7) panaikinus Direktyvą (ES) 2016/1148, taikymo sritis sektoriams, atsižvelgiant į 4–6 konstatuojamosiose dalyse išvardytas aplinkybes, turėtų būti praplėsta, kad apimtų platesnį ekonomikos veiklų spektrą. Todėl sektorių, kuriems taikoma Direktyva (ES) 2016/1148, sąrašas turėtų būti papildytas, kad direktyva būtų visapusiškai taikoma sektoriams ir paslaugoms, kurie yra gyvybiškai svarbūs pagrindinei visuomeninei ir ekonominei veiklai vidaus rinkoje. Taisyklės neturėtų skirtis priklausomai nuo to, ar subjektai yra esminių paslaugų operatoriai, ar skaitmeninių paslaugų teikėjai. Iš tiesų tokia diferenciacija yra pasenusi, nes neatspindi faktinės sektorių arba paslaugų svarbos visuomeninei ir ekonominei veiklai vidaus rinkoje;

(8) pagal Direktyvą (ES) 2016/1148 valstybės narės turėjo pareigą nustatyti, kurie subjektai atitinka esminių paslaugų operatoriams taikomus kriterijus (nustatymo procesas). Šiuo atžvilgiu siekiant pašalinti didelius valstybių narių skirtumus ir užtikrinti rizikos valdymo reikalavimų ir pareigų pranešti teisinį tikrumą visų subjektų 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 direktyvos taikymo sritį patenka visos vidutinės ir didelės įmonės, kaip apibrėžta Komisijos rekomendacijoje 2003/361/EB[15], veikiančios sektoriuose arba teikiančios atitinkamos rūšies paslaugas, kurioms taikoma ši direktyva. Nereikėtų reikalauti, kad valstybės narės sudarytų subjektų, atitinkančių šį visuotinai taikomą su dydžiu susijusį kriterijų, sąrašą;

(9) vis dėlto į šios direktyvos taikymo sritį taip pat turėtų patekti mažieji arba labai maži subjektai, atitinkantys tam tikrus kriterijus, iš kurių matyti, kad jie atlieka pagrindinį vaidmenį valstybių narių ekonomikoje ar visuomenėje arba konkrečiuose sektoriuose ar teikiant tam tikrų rūšių paslaugas. Valstybės narės turėtų turėti pareigą sudaryti tokių subjektų sąrašą ir pateikti jį Komisijai;

(10) Komisija, bendradarbiaudama su Bendradarbiavimo grupe, gali paskelbti labai mažoms ir mažosioms įmonėms taikomų kriterijų įgyvendinimo gaires;

(11) priklausomai nuo sektoriaus, kuriame veikia arba teikiamos paslaugos rūšies, subjektai, kurie patenka į šios direktyvos taikymo sritį, turėtų būti skirstomi į dvi – esminių ir svarbių subjektų – kategorijas. Skirstant į tas kategorijas, reikėtų atsižvelgti į sektoriaus arba paslaugos rūšies svarbą, taip pat į priklausomybės nuo kitų sektorių arba rūšių paslaugų svarbą. Tiek esminiams, tiek svarbiems subjektams turėtų būti taikomi tokie patys rizikos valdymo reikalavimai ir pareigos pranešti. Abiejų kategorijų subjektams taikomi priežiūros ir sankcijų režimai turėtų būti diferencijuojami siekiant užtikrinti tinkamą, viena vertus, reikalavimų ir pareigų ir,

[14] Srauto kontrolės protokolas (TLP) – tai priemonė, kurią naudodamas kuris nors asmuo dalijasi informacija, kad informuotų savo auditoriją apie bet kokius apribojimus, taikomus tolesnei šios informacijos sklaidai. Jis naudojamas beveik visose CSIRT bendruomenėse ir kai kuriuose informacijos analizės ir dalijimosi informacija centruose (ISAC).

[15] 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).

kita vertus, administracinės naštos, atsirandančios dėl atitikties priežiūros, pusiausvyrą;

(12) konkrečių sektorių teisės aktai ir priemonės gali padėti užtikrinti aukšto lygmens kibernetinį saugumą kartu visapusiškai atsižvelgiant į šių sektorių specifiką ir sudėtingumą. Jeigu pagal konkrečiam sektoriui taikomą Sąjungos teisės aktą reikalaujama, kad esminiai arba svarbūs subjektai priimtų kibernetinio saugumo rizikos valdymo priemones arba praneštų apie incidentus ar dideles kibernetines grėsmes, ir tokie reikalavimai bent jau turi lygiavertį poveikį kaip ir šioje direktyvoje nustatytos pareigos, turėtų būti taikomos tos konkretaus sektoriaus nuostatos, įskaitant priežiūrą ir vykdymo užtikrinimą reglamentuojančias nuostatas. Komisija gali priimti gaires, susijusias su *lex specialis* nuostatos įgyvendinimu. Šia direktyva nedraudžiama priimti papildomų konkretiems sektoriams taikomų Sąjungos aktų, kuriais reglamentuojamos kibernetinio saugumo rizikos valdymo priemonės ir pranešimo apie incidentus tvarka. Ši direktyva nedaro poveikio dabartiniams įgyvendinimo įgaliojimams, kurie Komisijai suteikti įvairiuose sektoriuose, įskaitant transporto ir energetikos sektorius;

(13) atsižvelgiant į tai, kiek ši direktyva yra susijusi su finansų sektoriaus subjektais, Europos Parlamento ir Tarybos reglamento XXXX/XXXX pasiūlymas[16] turėtų būti vertinamas kaip konkretaus sektoriaus Sąjungos teisės aktas. Reglamento XXXX/XXXX nuostatos, susijusios su informacinių ir ryšių technologijų (IRT) rizikos valdymo priemonėmis, IRT incidentų valdymu, ypač pranešimu apie incidentus, taip pat su skaitmeninės veiklos atsparumo testavimu, dalijimosi informacija tvarka ir trečiosios šalies IRT rizika, turėtų būti taikomos vietoj šioje direktyvoje nustatytų reikalavimų. Todėl valstybės narės šios direktyvos nuostatų dėl kibernetinio saugumo rizikos valdymo pareigų ir pareigų pranešti, dalijimosi informacija ir priežiūros bei vykdymo užtikrinimo neturėtų taikyti jokiems finansų sektoriaus subjektams, kuriems taikomas Reglamentas XXXX/XXXX. Kartu pagal šią direktyvą svarbu išlaikyti tvirtus ryšius su finansų sektoriumi ir užtikrinti, kad su juo būtų keičiamasi informacija. Šiuo tikslu Reglamentu XXXX/XXXX visoms finansų priežiūros institucijoms, Europos finansų sektoriaus priežiūros institucijoms (EPI) ir pagal Reglamentą XXXX/XXXX kompetentingoms nacionalinėms institucijoms leidžiama dalyvauti strateginėse politinėse diskusijose ir Bendradarbiavimo grupės techniniame darbe, taip pat keistis informacija bei bendradarbiauti su bendraisiais informaciniais centrais, paskirtais pagal šią direktyvą, ir su nacionalinėmis CSIRT. Pagal Reglamentą XXXX/XXXX kompetentingos institucijos, išsamius duomenis apie rimtus IRT incidentus taip pat turėtų perduoti pagal šią direktyvą paskirtiems bendriesiems informaciniams centrams. Be to, valstybės narės į savo kibernetinio saugumo strategijas turėtų toliau įtraukti finansų sektorių, o nacionalinės CSIRT savo veikloje gali aptarti finansų sektoriaus klausimus;

(14) atsižvelgiant į kibernetinio saugumo ir subjektų fizinio saugumo tarpusavio ryšius, reikėtų užtikrinti nuoseklų požiūrį tarp Europos Parlamento ir Tarybos direktyvos (ES) XXX/XXX[17] ir šios direktyvos. Kad pasiektų šį tikslą, valstybės narės turėtų užtikrinti, kad ypatingos svarbos subjektai pagal Direktyvą (ES) XXX/XXX būtų laikomi esminiais subjektais pagal šią direktyvą. Valstybės narės taip pat turėtų užtikrinti, kad jų kibernetinio saugumo strategijose būtų numatyta politikos sistema, kurioje būtų tvirčiau koordinuojama pagal šią direktyvą kompetentingos institucijos ir

16 *[įrašyti visą pavadinimą ir OL paskelbimo nuorodą, kai ji bus žinoma]*

17 *[įrašyti visą pavadinimą ir OL paskelbimo nuorodą, kai ji bus žinoma]*

pagal Direktyvą (ES) XXX/XXX kompetentingos institucijos veikla dalijantis informacija apie incidentus bei kibernetines grėsmes ir vykdant priežiūros užduotis. Institucijos pagal abi direktyvas turėtų bendradarbiauti ir keistis informacija, visų pirma atsižvelgiant į ypatingos svarbos subjektų nustatymą, kibernetines grėsmes, kibernetinio saugumo riziką, incidentus, darančius poveikį ypatingos svarbos subjektams, taip pat informacija apie kibernetinio saugumo priemones, kurių ėmėsi ypatingos svarbos subjektai. Pagal Direktyvą (ES) XXX/XXX kompetentingų institucijų prašymu pagal šią direktyvą kompetentingoms institucijoms turėtų būti leidžiama įgyvendinti savo priežiūros ir vykdymo užtikrinimo įgaliojimus subjektų, kurie įvardijami kaip ypatingos svarbos subjektai, atžvilgiu. Šiuo tikslu abi institucijos turėtų bendradarbiauti ir keistis informacija;

(15) patikimos, atsparios ir saugios domenų vardų sistemos (DNS) palaikymas ir išsaugojimas yra pagrindinis veiksnys užtikrinant interneto vientisumą ir yra labai svarbus jos nuolatiniam ir stabiliam veikimui, nuo kurio priklauso skaitmeninė ekonomika ir visuomenė. Todėl ši direktyva turėtų būti taikoma visiems DNS paslaugų teikėjams DNS keitimo grandinėje, įskaitant šakninio pavadinimo serverių operatorius, aukščiausio lygio domenų (TLD) vardų serverius, patikimo domenų vardų serverius ir rekursinius keitiklius;

(16) debesijos kompiuterijos paslaugos turėtų apimti skaitmenines paslaugas, kurios pagal poreikį suteikia plataus masto nuotolinę prieigą prie kintamo masto pritaikomos bendrų kompiuterijos išteklių bazės. Šie kompiuterijos ištekliai apima tokius išteklius, kaip tinklai, serveriai ar kita infrastruktūra, operacinės sistemos, programinė įranga, kaupikliai, taikomosios programos ir paslaugos. Debesijos kompiuterijos diegimo modeliai turėtų apimti privačią, viešą ir mišrią debesiją. Pirmiau minėti paslaugos ir diegimo modeliai turi tokią pat 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 ir naudojantis debesijos kompiuterijos paslaugų teikėju, galėtų būti apibūdinamas kaip administravimas pagal poreikį. Terminas „plataus masto nuotolinė prieiga“ naudojama 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, profesionaliuosius kompiuterius) naudojimas. Terminas „kintamo masto“ reiškia, kad siekdamas atsižvelgti į paklausos svyravimus, debesijos paslaugų teikėjas lanksčiai paskirsto kompiuterijos išteklius nepriklausomai nuo geografinės išteklių vietos. Terminas „pritaikoma bazė“ reiškia, kad siekiant sparčiai padidinti ir sumažinti tuos turimus kompiuterijos išteklius pagal darbo krūvį, tais ištekliais aprūpinama ir jie yra tiekiami atsižvelgiant į paklausą. Terminas „bendras“ reiškia, kad tie kompiuterijos ištekliai yra tiekiami įvairiems naudotojams, kurie dalijasi bendra prieiga prie paslaugos, tačiau tie ištekliai tvarkomi atskirai kiekvieno naudotojo atveju, nors paslauga yra teikiama naudojant tą pačią elektroninę įrangą. Terminas „paskirstytasis“ reiškia tuos kompiuterijos išteklius, kurie yra skirtinguose tinkliniuose kompiuteriuose ar prietaisuose ir kurie tarpusavyje bendrauja ir koordinuoja perduodami pranešimus;

(17) atsižvelgiant į novatoriškų technologijų ir naujų verslo modelių atsiradimą, tikimasi, kad rinkoje atsiras naujų debesijos kompiuterijos diegimo ir paslaugų 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);

(18) duomenų centro paslaugų teikėjų siūlomos paslaugos ne visada gali būti teikiamos debesijos kompiuterijos paslaugos forma. Atitinkamai, duomenų centrai ne visada gali priklausyti debesijos kompiuterijos infrastruktūrai. Siekiant valdyti visą riziką, kuri kyla tinklų ir informacinių sistemų saugumui, ši direktyva taip pat turėtų būti taikoma tokių duomenų centrų paslaugoms, kurios nėra debesijos kompiuterijos paslaugos. Taikant šią direktyvą, sąvoka „duomenų centro paslauga“ turėtų apimti teikiamą paslaugą, kuri apima struktūras arba struktūrų grupes, skirtas informacinių technologijų 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. sąvoka „duomenų centro paslauga“ netaikoma vidaus, korporatyviniams duomenų centrams, kurie priklauso atitinkamam subjektui ir yra eksploatuojami to subjekto reikmėms;

(19) pašto paslaugų teikėjams, kaip apibrėžta Europos Parlamento ir Tarybos direktyvoje 97/67/EB[18], taip pat greitojo pašto ir kurjerių paslaugų teikėjams ši direktyva turėtų būti taikoma, jeigu jie teikia paslaugas bent viename pašto paslaugų teikimo grandinės etape, ypač tvarkymo, rūšiavimo arba paskirstymo etape, įskaitant siuntų paėmimo paslaugas. Teikiamos vežimo paslaugos, kai jos nėra susijusios su vienu iš šių etapų, neturėtų patekti į pašto paslaugų apibrėžtį;

(20) šią didėjančią tarpusavio priklausomybę lemia vis labiau tarptautinio pobūdžio ir tarpusavyje priklausomas paslaugų teikimo tinklas, kuriame naudojami pagrindiniai visoje Sąjungoje esantys energetikos, transporto, skaitmeninės infrastruktūros, geriamojo vandens ir nuotekų, sveikatos, tam tikrų viešojo administravimo aspektų, taip pat kosmoso infrastruktūros objektai, atsižvelgiant į tai, kiek svarbus yra tam tikrų kosmoso paslaugų teikimas, 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 programas, arba kurie yra valdomi ar eksploatuojami Sąjungos vardu šių programų įgyvendinimo metu. Ši 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 pandemija parodė, kad mūsų vis labiau tarpusavyje priklausoma visuomenė yra pažeidžiama atsižvelgiant į mažai tikėtiną riziką;

(21) 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 daugiau nei vieną nacionalinę kompetentingą instituciją, atsakingą už užduočių, susijusių su esminių ir svarbių subjektų tinklų ir informacinių sistemų saugumu, vykdymą pagal šią direktyvą. Valstybės narės turėtų gebėti paskirti šį vaidmenį esamai institucijai;

(22) siekiant palengvinti tarpvalstybinį institucijų bendradarbiavimą ir ryšių palaikymą bei sudaryti sąlygas veiksmingai įgyvendinti šią direktyvą, būtina, kad kiekviena valstybė

[18] 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).

narė paskirtų nacionalinį bendrąjį informacinį centrą, atsakingą už klausimų, susijusių su tinklų ir informacinių sistemų saugumu, koordinavimą ir tarpvalstybinį bendradarbiavimą Sąjungos lygmeniu;

(23) kompetentingos institucijos arba CSIRT turėtų veiksmingai ir efektyviai iš subjektų gauti pranešimus apie incidentus. Bendriesiems informaciniams centrams turėtų būti pavesta persiųsti pranešimus apie incidentus kitų paveiktų valstybių narių bendriesiems informaciniams centrams. Valstybių narių institucijų lygmeniu siekiant užtikrinti vieną bendrą prieigą kiekvienoje valstybėje narėje, bendrieji informaciniai centrai taip pat turėtų gauti atitinkamą informaciją apie incidentus, susijusius su finansų sektoriaus subjektais iš pagal Reglamentą XXXX/XXXX kompetentingų institucijų, kurią jie turėtų turėti galimybę pagal šią direktyvą, kai tinkama, persiųsti atitinkamoms nacionalinėms kompetentingoms institucijoms arba CSIRT;

(24) valstybės narės turėtų būti tinkamai pasirengusios – turėti tiek techninių, tiek organizacinių pajėgumų, kad galėtų išvengti su tinklų ir informacinėmis sistemomis susijusių incidentų bei rizikos, juos nustatyti, į juos reaguoti ir sušvelninti jų poveikį. Todėl valstybės narės turėtų užtikrinti, kad jose būtų gerai veikiančios CSIRT, dar vadinamos reagavimo į kompiuterių incidentus tarnybos, atitinkančios esminius reikalavimus, kad būtų garantuoti veiksmingi bei suderinami incidentų bei rizikos valdymo pajėgumai ir užtikrintas veiksmingas bendradarbiavimas Sąjungos lygmeniu. Atsižvelgiant į pasitikėjimu grindžiamų santykių tarp subjektų ir CSIRT stiprinimą, tais atvejais, kai CSIRT veikia kompetentingoje institucijoje, valstybės narės turėtų apsvarstyti galimybę funkciniu požiūriu atskirti CSIRT vykdomas operatyvines užduotis, visų pirma susijusias su dalijimusi informacija ir parama subjektams, ir kompetentingų institucijų priežiūros veiklą;

(25) kalbant apie asmens duomenis pažymėtina, kad CSIRT turėtų turėti galimybę pagal Europos Parlamento ir Tarybos Reglamentą (ES) 2016/679[19] dėl asmens duomenų subjekto vardu ir jo prašymu pagal šią direktyvą imtis iniciatyvos patikrinti tinklų ir informacines sistemas, naudojamas jų paslaugoms teikti. Valstybės narės turėtų siekti užtikrinti vienodą visų sektorių CSIRT techninių pajėgumų lygį. Valstybės narės gali paprašyti Europos Sąjungos kibernetinio saugumo agentūros (ENISA) padėti kurti nacionalines CSIRT;

(26) 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;

(27) pagal Komisijos rekomendacijos (ES) 2017/1548 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes (planas)[20] priedą didelio masto incidentas turėtų reikšti incidentą, kuris turi reikšmingą poveikį ne mažiau kaip dviem valstybėms narėms arba į kurio sukeltą sutrikimą valstybė narė nepajėgia reaguoti. Priklausomai nuo jų priežasties ir poveikio, didelio masto incidentai gali stiprėti ir virsti plataus masto krizėmis, dėl kurių vidaus rinka negali tinkamai veikti. Atsižvelgiant į tai, kad tokie incidentai yra labai įvairaus masto ir dažniausiai tarpvalstybinio pobūdžio, valstybės narės ir atitinkamos ES institucijos, įstaigos ir

[19] 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).

[20] 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).

agentūros turėtų bendradarbiauti techniniu, operatyviniu ir politiniu lygmenimis, kad tinkamai koordinuotų atsaką visoje Sąjungoje;

(28) kadangi tinklų ir informacinių sistemų pažeidžiamumų išnaudojimas gali sukelti rimtus sutrikimus ir žalą, greitas šių pažeidžiamumų nustatymas ir jų ištaisymas yra svarbus veiksnys mažinant kibernetinio saugumo riziką. Todėl tokias sistemas kuriantys subjektai turėtų nustatyti atitinkamas procedūras, kurias taikant būtų šalinami aptikti pažeidžiamumai. Kadangi pažeidžiamumus dažnai aptinka ir apie juos praneša (atskleidžia) trečiosios šalys (pranešantieji subjektai), IRT produktų ar paslaugų gamintojas arba teikėjas taip pat turėtų nustatyti būtinas procedūras, pagal kurias iš trečiųjų šalių būtų gaunama informacija apie pažeidžiamumą. Šiuo atžvilgiu tarptautiniuose standartuose ISO/IEC 30111 ir ISO/IEC 29417 pateikiamos gairės atitinkamai dėl pažeidžiamumų šalinimo ir atskleidimo. Kalbant apie pažeidžiamumų atskleidimą pažymėtina, kad ypač svarbus pranešančiųjų subjektų ir IRT produktų ar paslaugų gamintojų arba teikėjų koordinavimas. Suderintas pažeidžiamumų atskleidimas yra struktūrinis procesas, per kurį organizacijoms pranešama apie pažeidžiamumus taip, kad joms būtų sudarytos sąlygos problemą nustatyti ir išspręsti prieš atskleidžiant išsamią informaciją apie pažeidžiamumus trečiosioms šalims arba visuomenei. Suderintas pažeidžiamumų atskleidimas taip pat turėtų apimti pranešančiojo subjekto ir organizacijos koordinavimą atsižvelgiant į taisymo laiką ir paskelbimą apie pažeidžiamumus;

(29) todėl valstybės narės turėtų imtis priemonių ir nustatyti atitinkamą nacionalinę politiką, kad palengvintų suderintą pažeidžiamumų atskleidimą. Šiuo atžvilgiu valstybės narės turėtų paskirti CSIRT, kad jos imtųsi koordinatoriaus vaidmens ir prireikus veiktų kaip pranešančiųjų subjektų ir IRT produktų arba paslaugų gamintojų ar teikėjų tarpininkas. CSIRT koordinatoriaus užduotys visų pirma turėtų apimti atitinkamų subjektų nustatymą ir susisiekimą su jais, pranešančiųjų subjektų rėmimą, derybas dėl informacijos atskleidimo tvarkaraščių ir pažeidžiamumų, kurie daro poveikį kelioms organizacijoms, valdymą (informacijos apie kelių šalių pažeidžiamumą atskleidimas). Jeigu pažeidžiamumai daro poveikį keliems IRT produktų ar paslaugų gamintojams arba teikėjams, įsisteigusiems daugiau nei vienoje valstybėje narėje, kiekvienos paveiktos valstybės narės paskirtosios CSIRT turėtų bendradarbiauti CSIRT tinkle;

(30) prieiga prie teisingos ir laiku pateikiamos informacijos apie pažeidžiamumus, kurie daro poveikį IRT produktams ir paslaugoms, padeda geriau valdyti kibernetinio saugumo riziką. Šiuo atžvilgiu viešai prieinamos informacijos apie pažeidžiamumus šaltiniai yra svarbi ne tik subjektų ir jų naudotojų, bet ir nacionalinių kompetentingų institucijų bei CSIRT priemonė. Dėl šios priežasties ENISA turėtų sukurti pažeidžiamumų registrą, kuriame esminiai ir svarbūs subjektai ir jų tiekėjai, taip pat subjektai, kurie nepatenka į šios direktyvos taikymo sritį, galėtų savanoriškai atskleisti pažeidžiamumus ir pateiktų informaciją apie pažeidžiamumą, kuri sudarytų sąlygas naudotojams imtis atitinkamų rizikos mažinimo priemonių;

(31) nors panašūs pažeidžiamumų registrai arba duomenų bazės jau yra sukurti, jų prieglobą vykdo ir juos tvarko subjektai, kurie nėra įsisteigę Sąjungoje. ENISA tvarkomas pažeidžiamumų registras padėtų užtikrinti didesnį paskelbimo proceso iki oficialaus pažeidžiamumų atskleidimo skaidrumą ir atsparumą panašių paslaugų teikimo sutrikimo arba nutraukimo atvejais. Siekdama išvengti veiksmų dubliavimo ir kuo didesnio papildomumo, ENISA turėtų išnagrinėti galimybę sudaryti struktūrinio bendradarbiavimo susitarimus su panašiais registrais trečiųjų šalių jurisdikcijose;

(32) Bendradarbiavimo grupė turėtų kas dvejus metus parengti darbo programą, įskaitant veiksmus, kurių grupė turi imtis, kad pasiektų savo tikslus ir įvykdytų užduotis. Pirmosios pagal šią direktyvą priimtos programos laikotarpis turėtų būti suderintas su paskutinės programos, priimtos pagal Direktyvą (ES) 2016/1148, laikotarpiu, kad būtų išvengta galimų grupės darbo sutrikimų;

(33) rengdama gairių dokumentus, Bendradarbiavimo grupė turėtų nuosekliai išsiaiškinti nacionalinius sprendimus ir patirtį, įvertinti Bendradarbiavimo grupės rezultatų poveikį nacionaliniam požiūriui, aptarti įgyvendinimo problemas ir suformuluoti konkrečias rekomendacijas, į kurias turėtų būti atsižvelgiama geriau įgyvendinant dabartines taisykles;

(34) Bendradarbiavimo grupė turėtų išlikti lanksčiu forumu ir sugebėti reaguoti į kintančius ir naujus politikos prioritetus bei problemas ir kartu atsižvelgti į prieinamus išteklius. Ji turėtų nuolat rengti bendrus susitikimus su atitinkamomis privačiomis suinteresuotosiomis šalimis iš visos Sąjungos, kad aptartų grupės vykdomą veiklą ir surinktų informacijos apie naujus politikos uždavinius. Siekdama didinti bendradarbiavimą Sąjungos lygmeniu, grupė turėtų apsvarstyti galimybę pakviesti jos veikloje dalyvauti kibernetinio saugumo politiką įgyvendinančias Sąjungos įstaigas ir agentūras, pavyzdžiui, Europos kovos su elektroniniu nusikalstamumu centrą (EC3), Europos Sąjungos aviacijos saugos agentūrą (EASA) ir Europos Sąjungos kosmoso programos agentūrą (EUSPA);

(35) kompetentingoms institucijoms ir CSIRT turėtų būti suteikti įgaliojimai dalyvauti pareigūnų iš kitų valstybių narių mainų programose siekiant pagerinti bendradarbiavimą. Kompetentingos institucijos turėtų imtis būtinų priemonių, kad pareigūnai iš kitų valstybių narių galėtų veiksmingai dalyvauti priimančiosios kompetentingos institucijos veikloje;

(36) pagal SESV 218 straipsnį Sąjunga, kai tinkama, turėtų sudaryti tarptautinius susitarimus su trečiosiomis šalimis ar tarptautinėmis organizacijomis, pagal kuriuos joms būtų leidžiama dalyvauti tam tikroje Bendradarbiavimo grupės ir CSIRT tinklo veikloje ir toks dalyvavimas būtų organizuojamas. Tokiuose susitarimuose turėtų būti užtikrinama tinkama duomenų apsauga;

(37) valstybės narės per esamus bendradarbiavimo tinklus, visų pirma per Europos ryšių palaikymo dėl kibernetinių krizių organizacinį tinklą („EU-CyCLONe“), CSIRT tinklą ir Bendradarbiavimo grupę, turėtų prisidėti kuriant Rekomendacijoje (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes numatytą ES reagavimo į kibernetinio saugumo krizes sistemą. „EU-CyCLONe“ ir CSIRT tinklas turėtų bendradarbiauti remdamiesi procedūrinėmis taisyklėmis, kuriomis apibrėžiami to bendradarbiavimo būdai. „EU-CyCLONe“ darbo tvarkos taisyklėse taip pat turėtų būti aptarti tinklo veikimo būdai, be kita ko, įskaitant vaidmenis, bendradarbiavimo metodus, sąveiką su kitais atitinkamais dalyviais ir dalijimosi informacija šablonus, taip pat ryšių palaikymo priemones, bet jais neapsiribojant. Siekdamos valdyti krizę Sąjungos lygmeniu, atitinkamos šalys turėtų kliautis integruoto politinio atsako į krizes mechanizmo (IPCR) nuostatomis. Komisija šiuo tikslu turėtų naudoti aukšto lygmens tarpsektorinį krizės koordinavimo procesą ARGUS. Jei krizė susijusi su svarbiais išorės arba bendros saugumo ir gynybos politikos (BSGP) aspektais, turėtų būti panaudotas Europos išorės veiksmų tarnybos (EIVT) reagavimo į krizę mechanizmas;

(38) šioje direktyvoje sąvoka „rizika“ turėtų reikšti potencialų praradimą arba sutrikimą, kurį sukėlė kibernetinio saugumo incidentas, ir ji turėtų būti išreikšta kaip tokio praradimo arba sutrikimo masto ir minėto incidento pasikartojimo derinys;

(39) šioje direktyvoje sąvoka „vos neįvykę incidentai“ turėtų reikšti įvykį, kuris galėjo sukelti potencialią žalą, tačiau faktiniam jo atsitikimui buvo sėkmingai užkirstas kelias;

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

(41) siekiant neužkrauti neproporcingos finansinės ir administracinės naštos esminiams ir svarbiems subjektams, kibernetinio saugumo rizikos valdymo reikalavimai turėtų būti proporcingi rizikai, kurią kelia atitinkama tinklų ir informacinė sistema, atsižvelgiant į tokių priemonių modernumą;

(42) esminiai ir svarbūs subjektai turėtų užtikrinti tinklų ir informacinių sistemų, kurias jie naudoja savo veikloje, saugumą. Tai visų pirma būtų privačios tinklų ir informacinės sistemos, kurias administruoja jų vidaus IT personalas arba kurių saugumas užtikrinamas veiklos ranga. Kibernetinio saugumo rizikos valdymo ir pranešimų teikimo reikalavimai pagal šią direktyvą turėtų būti taikomi atitinkamiems esminiams ir svarbiems subjektams, nepaisant to, ar jų tinklų ir informacinių sistemų techninę priežiūrą vykdo vidaus darbuotojai, ar rangovai;

(43) kibernetinio saugumo rizikos subjekto tiekimo grandinėje šalinimas ir subjekto santykiai su savo tiekėjais yra ypač svarbūs atsižvelgiant į incidentų paplitimą tais atvejais, kai subjektai tapo kibernetinių išpuolių aukomis ir kai piktavališki dalyviai galėjo pažeisti subjekto tinklų ir informacinių sistemų saugumą pasinaudodami pažeidžiamumais, taip darydami poveikį trečiųjų šalių produktams ir paslaugoms. Todėl subjektai turėtų įvertinti ir atsižvelgti į bendrą savo tiekėjų ir paslaugų teikėjų produktų ir kibernetinio saugumo praktikos, įskaitant jų saugaus tobulinimo procedūras, kokybę;

(44) kalbant apie paslaugų teikėjus pažymėtina, kad valdomi saugumo paslaugų teikėjai (MSSP) tokiose srityse kaip reagavimas į incidentus, skverbimosi testavimas, saugumo auditai ir konsultacijos atlieka itin svarbų vaidmenį padėdami subjektams nustatyti incidentus ir į juos reaguoti. Tačiau tie MSSP taip pat buvo pačių kibernetinių išpuolių taikiniai, o juos glaudžiai integravus į operatorių veiklą kyla tam tikra kibernetinio saugumo rizika. Todėl subjektai, atrinkdami MSSP, turėtų veikti atidžiau;

(45) subjektai taip pat turėtų mažinti kibernetinio saugumo riziką, kylančią dėl jų sąveikos ir santykių su kitomis suinteresuotosiomis šalimis platesnėje ekosistemoje. Visų pirma 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 subjektų veiklai, kai jie priklauso nuo duomenų transformavimo ir duomenų analizės paslaugų, kurias teikia trečiosios šalys, subjektai turėtų imtis visų tinkamų kibernetinio saugumo priemonių;

(46) siekiant toliau mažinti pagrindinę tiekimo grandinės riziką ir padėti subjektams, veikiantiems sektoriuose, kuriems taikoma ši direktyva, tinkamai valdyti su tiekimo grandine ir tiekėjais susijusią kibernetinio saugumo riziką, Bendradarbiavimo grupė, kurioje dalyvauja atitinkamos nacionalinės institucijos, bendradarbiaudama su Komisija ir ENISA, turėtų atlikti suderintus sektorių tiekimo grandinės rizikos vertinimus, kaip jau buvo padaryta 5G tinklų atveju pagal Rekomendaciją (ES) 2019/534 dėl 5G tinklų kibernetinio saugumo[21], siekiant nustatyti sektorius, kurie yra ypatingos svarbos IRT paslaugos, sistemos ar produktai, atitinkamos grėsmės ir pažeidžiamumai;

(47) atliekant tiekimo grandinės 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 saugumo visoje ES suderintame rizikos vertinime ir ES 5G kibernetinio saugumo priemonių rinkinyje, dėl kurio susitarė Bendradarbiavimo grupė. Siekiant išsiaiškinti, kurioms tiekimo grandinėms turėtų būti taikomas koordinuotas rizikos vertinimas, reikėtų atsižvelgti į šiuos kriterijus: i) kokiu mastu esminiai ir svarbūs subjektai naudojasi konkrečiomis ypatingos svarbos IRT paslaugomis, sistemomis ar produktais ir nuo jų priklauso; ii) konkrečių ypatingos svarbos IRT paslaugų, sistemų ar produktų svarbą vykdant ypatingos svarbos arba neskelbtinas funkcijas, įskaitant asmens duomenų tvarkymą; iii) alternatyvių IRT paslaugų, sistemų ar produktų prieinamumą; iv) visos IRT paslaugų, sistemų ar produktų tiekimo grandinės atsparumą sutrikimams ir v) atsirandančių IRT paslaugų, sistemų ar produktų atveju, jų galimą būsimą svarbą subjektų veiklai;

(48) siekiant supaprastinti viešųjų elektroninių ryšių tinklų ar viešai prieinamų elektroninių ryšių paslaugų teikėjams ir patikimumo užtikrinimo paslaugų teikėjams taikomas teisines pareigas, susijusias su jų tinklų ir informacinių sistemų saugumu, taip pat sudaryti sąlygas tiems subjektams ir jų atitinkamoms kompetentingoms institucijoms pasinaudoti šioje direktyvoje nustatyta teisine sistema (įskaitant CSIRT, atsakingą už rizikos ir incidentų valdymą, kompetentingų institucijų ir įstaigų dalyvavimą Bendradarbiavimo grupės ir CSIRT tinklo veikloje, paskyrimą), jie turėtų būti įtraukti į šios direktyvos taikymo sritį. Todėl atitinkamos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014[22] ir Europos Parlamento ir Tarybos direktyvos (ES) 2018/1972[23] nuostatos, susijusios su saugumo ir pranešimo reikalavimo nustatymu šių rūšių subjektams, turėtų būti panaikintos. Taisyklės dėl pareigų pranešti neturėtų daryti poveikio Reglamentui (ES) 2016/679 ir Europos Parlamento ir Tarybos direktyvai 2002/58/EB[24];

(49) kai tinkama ir siekiant išvengti nereikalingo trikdymo, kompetentingos institucijos, atsakingos už šios direktyvos nuostatų, susijusių su priežiūra ir vykdymo užtikrinimu, turėtų toliau naudotis galiojančiomis nacionalinėmis gairėmis ir nacionalinės teisės

---

21 2019 m. kovo 26 d. Komisijos rekomendacija (ES) 2019/534 dėl 5G tinklų kibernetinio saugumo (OL L 88, 2019 3 29, p. 42).

22 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).

23 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).

24 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).

aktais, priimtais siekiant į nacionalinę teisę perkelti taisykles, susijusias su Direktyvos (ES) 2018/1972 40 straipsnio 1 dalyje nustatytomis saugumo priemonėmis, taip pat tos direktyvos 40 straipsnio 2 dalies reikalavimus dėl parametrų, susijusių su incidento svarba;

(50) atsižvelgiant į didėjančią su numeriu nesiejamo asmenų tarpusavio ryšio paslaugų svarbą, būtina užtikrinti, kad tokioms paslaugoms, atsižvelgiant į jų specifinį pobūdį ir ekonominę svarbą, taip pat būtų taikomi tinkami saugumo reikalavimai. Todėl tokių paslaugų teikėjai taip pat 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 valdyti 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, kurias teikiant naudojami numeriai ir kurias teikiant faktiškai nekontroliuojamas signalų perdavimas;

(51) vidaus rinka labiau nei kada nors anksčiau priklauso nuo interneto veikimo. Beveik visų pagrindinių ir svarbių subjektų paslaugos priklauso nuo internetu teikiamų paslaugų. Siekiant užtikrinti sklandų esminių ir svarbių subjektų teikiamų paslaugų teikimą, svarbu, kad viešuosiuose elektroninių ryšių tinkluose, pavyzdžiui, interneto magistralėse ar povandeniniuose ryšių kabeliuose, būtų įdiegtos tinkamos kibernetinio saugumo priemonės ir būtų pranešama apie su jomis susijusius incidentus;

(52) kai tinkama, subjektai turėtų informuoti savo paslaugų gavėjus apie konkrečias ir dideles grėsmes ir apie priemones, kurių jie gali imtis, kad sumažintų jiems kylančią riziką. Reikalavimas informuoti tuos gavėjus apie tokias grėsmes neturėtų atleisti subjektų nuo pareigos savo sąskaita imtis tinkamų ir neatidėliotinų priemonių, kad būtų užkirstas kelias kibernetinėms grėsmėms arba jos būtų ištaisytos ir atkurtas įprastas paslaugos saugumo lygis. Tokia informacija apie saugumo grėsmes gavėjams turėtų būti teikiama nemokamai;

(53) visų pirma viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai turėtų informuoti paslaugų gavėjus apie konkrečias ir dideles kibernetines grėsmes ir priemones, kurių jie gali imtis savo ryšių saugumui užtikrinti, pavyzdžiui, naudodami konkrečių rūšių programinę įrangą arba šifravimo technologijas;

(54) siekiant užtikrinti elektroninių ryšių tinklų ir paslaugų saugumą, turėtų būti skatinama naudoti šifravimą, visų pirma ištisinį šifravimą, ir, kai būtina, jis turėtų būti privalomas tokių paslaugų ir tinklų teikėjams laikantis pritaikytosios duomenų apsaugos ir standartizuotosios duomenų apsaugos principų 18 straipsnio tikslais. Ištisinio šifravimo naudojimas turėtų derėti su valstybių narių įgaliojimais užtikrinti savo esminių saugumo interesų apsaugą ir visuomenės saugumą ir leisti tirti, atskleisti nusikalstamas veikas ir vykdyti baudžiamąjį persekiojimą už jas laikantis Sąjungos teisės. Sprendimai, susiję su teisėta prieiga prie informacijos ištisiniuose šifruotuose ryšiuose, turėtų išlaikyti šifravimo veiksmingumą apsaugant ryšių privatumą ir saugumą, kartu užtikrinant veiksmingą atsaką į nusikalstamumą;

(55) šia direktyva nustatomas dviejų etapų pranešimų apie incidentus teikimo metodas, siekiant užtikrinti tinkamą pusiausvyrą tarp, viena vertus, greito pranešimų teikimo, kuris padeda sumažinti galimą incidentų plitimą ir suteikia galimybę subjektams prašyti paramos, ir, kita vertus, išsamių pranešimų, kuriuose atsižvelgiama į vertingą su pavieniais incidentais susijusią patirtį ir ilgainiui didinamas atskirų įmonių ir visų

sektorių atsparumas kibernetinėms grėsmėms. Jei subjektai sužino apie incidentą, jie turėtų pateikti pradinį pranešimą per 24 valandas, o galutinę ataskaitą privalo pateikti ne vėliau kaip per vieną mėnesį po to pranešimo. Pradiniame pranešime turėtų būti pateikta tik informacija, kurios būtinai reikia, kad kompetentingos institucijos žinotų apie incidentą, o subjektas prireikus galėtų kreiptis pagalbos. Tokiame pranešime, kai taikytina, turėtų būti nurodyta, ar incidentą, kaip įtariama, sukėlė neteisėti arba piktavališki veiksmai. Valstybės narės turėtų užtikrinti, kad dėl reikalavimo pateikti šį pradinį pranešimą teikiančio subjekto ištekliai nebūtų nukreipti nuo veiklos, susijusios su incidentų valdymu, kuriam turėtų būti teikiama pirmenybė. Siekdamos toliau užkirsti kelią tam, kad vykdant pareigas pranešti apie incidentus ištekliai nebūtų nukreipiami nuo reagavimo į incidentus valdymo arba kitaip nebūtų pakenkta subjektų pastangoms šioje srityje, valstybės narės taip pat turėtų nustatyti, kad tinkamai pagrįstais atvejais ir susitarus su kompetentingomis institucijomis arba CSIRT atitinkamas subjektas gali nukrypti nuo 24 valandų termino pradiniam pranešimui ir vieno mėnesio termino galutinės ataskaitos pateikimui;

(56) esminiai ir svarbūs 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 našta ir gali kilti neaiškumų dėl tokių pranešimų formos ir procedūrų. Atsižvelgiant į tai ir siekiant supaprastinti pranešimų apie saugumo incidentus teikimą, valstybės narės turėtų sukurti *vieną bendrą prieigą* visiems pranešimams, kuriuos reikalaujama pateikti pagal šią direktyvą ir kitus Sąjungos teisės aktus, pavyzdžiui, Reglamentą (ES) 2016/679 ir Direktyvą 2002/58/EB. ENISA, bendradarbiaudama su Bendradarbiavimo grupe, turėtų parengti bendrus pranešimo šablonus, pateikdama gaires, kuriomis būtų supaprastinta ir racionalizuota pagal Sąjungos teisę reikalaujama pranešimų teikimo informacija ir sumažinta bendrovėms tenkanti našta;

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

(58) daugeliu atvejų dėl incidentų kyla pavojus asmens duomenų saugumui. Tokiomis aplinkybėmis kompetentingos institucijos turėtų bendradarbiauti ir keistis informacija visais svarbiais klausimais su duomenų apsaugos institucijomis ir priežiūros institucijomis pagal Direktyvą 2002/58/EB;

(59) siekiant užtikrinti DNS saugumą, stabilumą ir atsparumą, būtina turėti tikslias ir išsamias domenų vardų ir registracijos duomenų (vadinamųjų WHOIS duomenų) bazes ir suteikti teisėtą prieigą prie tokių duomenų, o tai savo ruožtu prisideda prie aukšto bendro kibernetinio saugumo lygio Sąjungoje. Kai tvarkomi asmens duomenys, toks tvarkymas turi atitikti Sąjungos duomenų apsaugos teisės aktus;

(60) šių duomenų prieinamumas ir galimybė laiku su jais susipažinti valdžios institucijoms, įskaitant kompetentingas institucijas pagal Sąjungos ar nacionalinę teisę nusikalstamų veikų prevencijos, tyrimo ar baudžiamojo persekiojimo už jas tikslais, CERT, CSIRT ir elektroninių ryšių tinklų ir paslaugų teikėjams ir tų klientų vardu veikiančių kibernetinio saugumo technologijų ir paslaugų teikėjams tiek, kiek tai susiję su jų

klientų duomenimis, yra labai svarbūs siekiant užkirsti kelią piktnaudžiavimui domenų vardų sistema ir su juo kovoti, visų pirma siekiant užkirsti kelią kibernetinio saugumo incidentams, juos nustatyti ir į juos reaguoti. Tokia prieiga turėtų atitikti Sąjungos duomenų apsaugos teisę tiek, kiek ji susijusi su asmens duomenimis;

(61) siekiant užtikrinti tikslių ir išsamių domenų vardų registracijos duomenų prieinamumą, aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys aukščiausio lygio domenų vardų registravimo paslaugas (vadinamieji registratoriai), turėtų rinkti domenų vardų registracijos duomenis ir užtikrinti jų vientisumą ir prieinamumą. Visų pirma, aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys aukščiausio lygio domenų vardų registravimo paslaugas, turėtų nustatyti politiką ir procedūras, skirtas tiksliems ir išsamiems registracijos duomenims rinkti ir saugoti, taip pat užkirsti kelią netiksliems registracijos duomenims ir juos ištaisyti pagal Sąjungos duomenų apsaugos taisykles;

(62) aukščiausio lygio domenų vardų registrai ir jiems skirtas domenų vardų registravimo paslaugas teikiantys subjektai turėtų viešai skelbti domenų vardų registracijos duomenis, kuriems netaikomos Sąjungos duomenų apsaugos taisyklės, pavyzdžiui, duomenis, susijusius su juridiniais asmenimis[25]. Pagal Sąjungos duomenų apsaugos teisę aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys aukščiausio lygio domenų vardų registravimo paslaugas, taip pat turėtų suteikti teisėtą prieigą prie fizinių asmenų konkrečių domenų vardų registracijos duomenų. Valstybės narės turėtų užtikrinti, kad aukščiausio lygio domenų vardų registrai ir jų domenų vardų registravimo paslaugas teikiantys subjektai nepagrįstai nedelsdami atsakytų į teisėtų prieigos siekiančių subjektų prašymus atskleisti domenų vardų registracijos duomenis. Aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys jiems domenų vardų registravimo paslaugas, turėtų nustatyti registracijos duomenų skelbimo ir atskleidimo politiką ir procedūras, įskaitant susitarimus dėl paslaugų lygio, skirtus tvarkyti teisėtų prieigos siekiančių subjektų prašymus suteikti prieigą. Prieigos procedūra taip pat gali 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 priimti tokių procedūrų gaires, nepažeisdama Europos duomenų apsaugos valdybos kompetencijos;

(63) visi esminiai ir svarbūs subjektai, kuriems taikoma ši direktyva, turėtų priklausyti valstybės narės, kurioje jie teikia savo paslaugas, jurisdikcijai. Jeigu subjektas teikia paslaugas daugiau nei vienoje valstybėje narėje, jis turėtų priklausyti atskirai ir lygiagrečiai kiekvienos iš šių valstybių narių jurisdikcijai. Šių valstybių narių kompetentingos institucijos turėtų bendradarbiauti, teikti viena kitai savitarpio pagalbą ir prireikus vykdyti bendrus priežiūros veiksmus;

(64) siekiant atsižvelgti į DNS paslaugų teikėjų, aukščiausio lygio domenų vardų registrų, turinio teikimo tinklo teikėjų, debesijos kompiuterijos paslaugų teikėjų, duomenų centrų paslaugų teikėjų ir skaitmeninių paslaugų teikėjų tarpvalstybinį paslaugų ir veiklos pobūdį, jurisdikciją šių 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

[25] EUROPOS PARLAMENTO IR TARYBOS REGLAMENTO (ES) 2016/679 14 konstatuojamoji dalis, pagal kurią „šis reglamentas netaikomas asmens duomenų, susijusių su juridiniais asmenimis ir visų pirma įmonėmis, įsteigtomis kaip juridiniai asmenys, tvarkymui, įskaitant juridinio asmens vardą, pavardę, formą ir juridinio asmens kontaktinius duomenis“.

veiksmingą veiklos vykdymą per nuolatines struktūras. Teisinė tokių struktūrų forma, nepaisant to, ar tai filialas ar patronuojamoji įmonė, turinti juridinio asmens statusą, tuo požiūriu 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. Pagrindinė buveinė turėtų būti vieta, kurioje Sąjungoje priimami su kibernetinio saugumo rizikos valdymo priemonėmis susiję sprendimai. Paprastai ji sutampa su įmonių centrinės administracijos vieta Sąjungoje. Jei tokie sprendimai nepriimami Sąjungoje, turėtų būti laikoma, kad pagrindinė buveinė yra valstybėse narėse, kuriose subjektas turi padalinį, kuriame dirba daugiausia darbuotojų Sąjungoje. Jeigu paslaugas teikia įmonių grupė, pagrindinė kontroliuojančiosios įmonės buveinė turėtų būti laikoma pagrindine įmonių grupės buveine;

(65) tais atvejais, kai paslaugas Sąjungoje siūlo DNS paslaugų teikėjas, aukščiausio lygio domenų vardų registras, turinio teikimo tinklo paslaugų teikėjas, debesijos kompiuterijos paslaugų teikėjas, duomenų centro paslaugų teikėjas ir skaitmeninių paslaugų teikėjas, kurie nėra įsisteigę Sąjungoje, tokie tiekėjai turėtų paskirti atstovą. Siekiant nustatyti, ar toks subjektas siūlo paslaugas Sąjungoje, reikėtų įvertinti, ar akivaizdu, kad subjektas ketina siūlyti paslaugas asmenims vienoje ar keliose valstybėse narėse. Vien to, kad Sąjungoje prieinama subjekto ar tarpininko interneto svetainė arba e. pašto adresas ir kiti kontaktiniai duomenys arba kad vartojama kalba, kuri paprastai vartojama trečiojoje šalyje, 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 kita 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 jo pareigas pagal šią direktyvą, įskaitant pranešimą apie incidentus;

(66) jeigu pagal šios direktyvos nuostatas keičiamasi informacija, kuri laikoma įslaptinta pagal nacionalinę arba Sąjungos teisę, apie ją pranešama arba ja kitaip dalijamasi, turėtų būti taikomos atitinkamos konkrečios įslaptintos informacijos tvarkymo taisyklės;

(67) kadangi kibernetinės grėsmės tampa vis sudėtingesnės ir painesnės, geros aptikimo 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 grėsmėms virsti tikrais incidentais ir sudaro sąlygas subjektams geriau suvaldyti incidentų poveikį ir veiksmingiau atkurti veiklą. Nesant gairių Sąjungos lygmeniu, atrodo, kad keli veiksniai trukdo dalytis žvalgybos informacija, visų pirma netikrumas dėl suderinamumo su konkurencijos ir atsakomybės taisyklėmis;

(68) subjektai turėtų būti skatinami bendrai naudotis savo asmeninėmis žiniomis ir praktine patirtimi strateginiu, taktiniu ir veiklos lygmenimis, kad sustiprintų savo gebėjimus tinkamai vertinti, stebėti kibernetines grėsmes, apsisaugoti nuo jų ir į jas reaguoti. Todėl būtina sudaryti sąlygas Sąjungos lygmeniu kurti savanoriško keitimosi informacija mechanizmus. Šiuo tikslu valstybės narės turėtų aktyviai remti ir skatinti atitinkamus subjektus, kuriems netaikoma ši direktyva, dalyvauti tokiuose keitimosi

informacija mechanizmuose. Tie mechanizmai turėtų būti taikomi visapusiškai laikantis Sąjungos konkurencijos taisyklių ir Sąjungos teisės nuostatų dėl duomenų apsaugos;

(69) subjektų, valdžios institucijų, CERT, CSIRT ir saugumo technologijų bei paslaugų teikėjų vykdomas asmens duomenų tvarkymas tiek, kiek tai tikrai būtina ir proporcinga siekiant užtikrinti tinklų ir informacijos saugumą, turėtų būti teisėtas atitinkamo duomenų valdytojo interesas, kaip nurodyta Reglamente (ES) 2016/679. Tai turėtų apimti priemones, susijusias su incidentų prevencija, nustatymu, analize ir reagavimu į juos, informuotumo apie konkrečias kibernetines grėsmes didinimo priemones, keitimąsi informacija atkuriant pažeidžiamumą ir suderintai jį atskleidžiant, taip pat savanorišką keitimąsi informacija apie tuos incidentus, kibernetines grėsmes ir pažeidžiamumus, užvaldymo rodiklius, taktiką, metodus ir procedūras, kibernetinio saugumo perspėjimus ir konfigūracijos priemones. Taikant tokias priemones gali prireikti tvarkyti šių rūšių asmens duomenis: IP adresus, universaliuosius išteklių adresus (URL), domenų vardus ir e. pašto adresus;

(70) siekiant sustiprinti priežiūros įgaliojimus ir veiksmus, padedančius užtikrinti veiksmingą reikalavimų laikymąsi, šioje direktyvoje turėtų būti nustatytas būtiniausias priežiūros veiksmų ir priemonių, kuriomis kompetentingos institucijos galėtų prižiūrėti esminius ir svarbius subjektus, sąrašas. Be to, šioje direktyvoje turėtų būti nustatyta atskira esminių ir svarbių subjektų priežiūros tvarka, siekiant užtikrinti teisingą tiek subjektų, tiek kompetentingų institucijų pareigų pusiausvyrą. Taigi esminiams subjektams turėtų būti taikoma visavertė priežiūros tvarka (*ex ante* ir *ex post*), o svarbiems subjektams turėtų būti taikoma negriežta priežiūros tvarka, t. y. tik *ex post*. Pastaruoju atveju tai reiškia, kad svarbūs subjektai neturėtų sistemingai dokumentuoti atitikties kibernetinio saugumo rizikos valdymo reikalavimams, o kompetentingos institucijos turėtų įgyvendinti reaktyvųjį *ex post* požiūrį į priežiūrą, todėl neturėtų turėti bendros pareigos prižiūrėti tuos subjektus;

(71) kad vykdymo užtikrinimas būtų veiksmingas, turėtų būti parengtas būtinas administracinių sankcijų už šioje direktyvoje nustatytų kibernetinio saugumo rizikos valdymo ir pranešimo pareigų pažeidimą sąrašas, kuriuo būtų sukurta aiški ir nuosekli tokių sankcijų sistema visoje Sąjungoje. Reikėtų deramai atsižvelgti į pažeidimo pobūdį, rimtumą ir trukmę, faktiškai padarytą žalą ar patirtus nuostolius arba galimą žalą ar nuostolius, kurie galėjo būti patirti, į tai, ar pažeidimas buvo padarytas tyčia, ar dėl aplaidumo, veiksmus, kurių imtasi siekiant užkirsti kelią patirtai žalai ir (arba) nuostoliams arba juos sumažinti, atsakomybės laipsnį ar bet kokius atitinkamus ankstesnius pažeidimus, bendradarbiavimo su kompetentinga institucija laipsnį ir visas kitas atsakomybę sunkinančias arba švelninančias aplinkybes. Skiriant sankcijas, įskaitant administracines baudas, turėtų būti taikomos tinkamos procedūrinės apsaugos priemonės pagal bendruosius Sąjungos teisės principus ir Europos Sąjungos pagrindinių teisių chartiją, įskaitant veiksmingą teisminę apsaugą ir tinkamą procesą;

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

(73) jei administracinės baudos skiriamos įmonei, tais tikslais įmonė turėtų būti suprantama kaip įmonė, apibrėžta SESV 101 ir 102 straipsniuose. Jei administracinės baudos skiriamos asmenims, kurie nėra įmonė, svarstydama, koks būtų tinkamas baudos dydis, priežiūros 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;

(74) 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 Teisingumo Teismas;

(75) kai šia direktyva administracinės sankcijos nėra suderintos arba kai tai yra būtina kitais atvejais, pavyzdžiui, kai šiurkščiai pažeidžiamos šioje direktyvoje nustatytos pareigos, valstybės narės turėtų įgyvendinti sistemą, pagal kurią numatomos veiksmingos, proporcingos ir atgrasomosios sankcijos. Tokių sankcijų – baudžiamųjų ar administracinių – pobūdis turėtų būti nustatytas valstybės narės teisėje;

(76) siekiant dar labiau sustiprinti sankcijų, taikomų už pagal šią direktyvą nustatytų pareigų pažeidimus, veiksmingumą ir atgrasomumą, kompetentingoms institucijoms turėtų būti suteikti įgaliojimai taikyti sankcijas, kurias sudaro sertifikavimo ar leidimo sustabdymas, susijęs su dalies ar visų esminių subjektų teikiamų paslaugų teikimu, ir laikinas draudimas fiziniam asmeniui eiti vadovaujamas pareigas. Atsižvelgiant į tokių sankcijų griežtumą ir poveikį subjektų veiklai ir galiausiai jų vartotojams, jos turėtų būti taikomos tik proporcingai pažeidimo sunkumui ir atsižvelgiant į konkrečias kiekvieno atvejo aplinkybes, įskaitant tai, ar pažeidimas padarytas tyčia, ar dėl aplaidumo, veiksmus, kurių imtasi siekiant užkirsti kelią patirtai žalai ir (arba) nuostoliams arba juos sumažinti. Tokios sankcijos turėtų būti taikomos tik kaip *ultima ratio*, t. y. tik po to, kai išnaudojami kiti šioje direktyvoje nustatyti atitinkami vykdymo užtikrinimo veiksmai, ir tik tol, kol subjektai, kuriems jos taikomos, imasi reikiamų veiksmų trūkumams pašalinti arba kompetentingos institucijos, kuriai taikytos tokios sankcijos, reikalavimams įvykdyti. Skiriant tokias sankcijas, turėtų būti taikomos tinkamos procedūrinės apsaugos priemonės pagal bendruosius Sąjungos teisės principus ir Europos Sąjungos pagrindinių teisių chartiją, įskaitant veiksmingą teisminę apsaugą, tinkamą procesą, nekaltumo prezumpciją ir teisę į gynybą;

(77) šia direktyva turėtų būti nustatytos kompetentingų institucijų ir priežiūros institucijų bendradarbiavimo taisyklės pagal Reglamentą (ES) 2016/679, siekiant kovoti su pažeidimais, susijusiais su asmens duomenimis;

(78) šia direktyva turėtų būti siekiama užtikrinti aukšto lygio atsakomybę už kibernetinio saugumo rizikos valdymo priemones ir pareigas pranešti organizacijų lygmeniu. Dėl šių priežasčių subjektų, kuriems taikoma ši direktyva, valdymo organai turėtų patvirtinti kibernetinio saugumo rizikos priemones ir prižiūrėti jų įgyvendinimą;

(79) turėtų būti nustatytas tarpusavio vertinimo mechanizmas, pagal kurį valstybių narių paskirti ekspertai galėtų įvertinti, kaip įgyvendinama kibernetinio saugumo politika, įskaitant valstybių narių pajėgumų lygį ir turimus išteklius;

(80) siekiant atsižvelgti į naujas kibernetines grėsmes, technologinę plėtrą ar sektorių ypatumus, pagal SESV 290 straipsnį Komisijai turėtų būti deleguoti įgaliojimai priimti aktus dėl elementų, susijusių su rizikos valdymo priemonėmis, kurių reikalaujama pagal šią direktyvą. Komisijai taip pat turėtų būti suteikti įgaliojimai priimti deleguotuosius aktus, kuriais būtų nustatyta, kokių kategorijų esminiams subjektams reikia gauti sertifikatą ir pagal kurias konkrečias Europos kibernetinio saugumo

sertifikavimo schemas. 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 nustatytais principais[26]. Visų pirma, siekiant užtikrinti vienodas galimybes dalyvauti atliekant su deleguotaisiais aktais susijusį parengiamąjį darbą, Europos Parlamentas ir Taryba visus dokumentus turėtų gauti tuo pačiu metu kaip ir valstybių narių ekspertai, o jų ekspertams turėtų būti sistemingai suteikiama galimybė dalyvauti Komisijos ekspertų grupių, kurios atlieka su deleguotaisiais aktais susijusį parengiamąjį darbą, posėdžiuose;

(81) siekiant užtikrinti vienodas atitinkamų šios direktyvos nuostatų, susijusių su Bendradarbiavimo grupės veikimui būtina procedūrine tvarka, techniniais elementais, susijusiais su rizikos valdymo priemonėmis arba su informacijos rūšimi, pranešimų apie incidentus forma ir tvarka, įgyvendinimo sąlygas, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai. Tais įgaliojimais turėtų būti naudojamasi laikantis Europos Parlamento ir Tarybos reglamento (ES) Nr. 182/2011[27];

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

(83) kadangi šios direktyvos tikslo, t. y. užtikrinti aukštą bendrą kibernetinio saugumo lygį 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;

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

PRIĖMĖ ŠIĄ DIREKTYVĄ:

I SKYRIUS

Bendrosios nuostatos

1 straipsnis

Dalykas

1. Šia direktyva nustatomos priemonės, kuriomis siekiama užtikrinti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje.

[26] OL L 123, 2016 5 12, p. 1.

[27] 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).

2. Todėl šia direktyva nustatomos:

(a) valstybių narių pareigos priimti nacionalines kibernetinio saugumo strategijas, paskirti kompetentingas nacionalines institucijas, bendruosius informacinius centrus ir reagavimo į kompiuterių saugumo incidentus tarnybas (CSIRT);

b) kibernetinio saugumo rizikos valdymo pareigos ir pareigos pranešti, taikomos subjektams, kurie I priede įvardijami kaip esminiai subjektai, ir subjektams, kurie II priede įvardijami kaip svarbūs subjektai;

(c) pareigos dalytis kibernetinio saugumo informacija.

2 straipsnis

Taikymo sritis

1. Ši direktyva taikoma viešiesiems ir privatiesiems subjektams, kurie I priede įvardijami kaip esminiai subjektai, o II priede – kaip svarbūs subjektai. Ši direktyva netaikoma subjektams, kurie atitinka labai mažų ir mažųjų įmonių apibrėžtį pagal Komisijos rekomendaciją 2003/361/EB[28].

2. Tačiau, nepaisant subjektų dydžio, ši direktyva taikoma I ir II prieduose nurodytiems subjektams, kai:

(a) paslaugas teikia vienas iš toliau išvardytų subjektų:

i) viešųjų elektroninių ryšių tinklai arba viešai prieinamų elektroninių ryšių paslaugų teikėjai, nurodyti I priedo 8 punkte;

ii) patikimumo užtikrinimo paslaugų teikėjai, nurodyti I priedo 8 punkte;

iii) aukščiausio lygio domenų vardų registrai ir domenų vardų sistemos (DNS) paslaugų teikėjai, nurodyti I priedo 8 punkte;

b) subjektas yra viešojo administravimo subjektas, kaip apibrėžta 4 straipsnio 23 punkte;

c) subjektas yra vienintelis paslaugos teikėjas valstybėje narėje;

d) potencialus paslaugos, kurią teikia subjektas, sutrikimas galėtų turėti poveikį viešajam saugumui, visuomenės saugumui arba visuomenės sveikatai;

e) potencialus paslaugos, kurią teikia subjektas, sutrikimas galėtų kelti sisteminę riziką visų pirma sektoriuose, kuriuose toks sutrikimas galėtų turėti tarpvalstybinį poveikį;

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

[28] 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).

g) nustatoma, kad subjektas yra ypatingos svarbos pagal Europos Parlamento ir Tarybos direktyvą (ES) XXXX/XXXX[29] [Ypatingos svarbos subjektų atsparumo direktyva] arba kad subjektas yra lygiavertis ypatingos svarbos subjektui pagal tos direktyvos 7 straipsnį.

Valstybės narės sudaro pagal b–f punktus nustatytų subjektų sąrašą ir pateikia jį Komisijai ne vėliau kaip praėjus [6 mėnesiams nuo perkėlimo į nacionalinę teisę termino pabaigos]. Valstybės narės nuolat ir ne rečiau kaip kas dvejus metus peržiūri sąrašą ir, kai tinkama, jį atnaujina.

3. Ši direktyva nedaro poveikio valstybių narių kompetencijai viešojo saugumo, gynybos ir nacionalinio saugumo palaikymo pagal Sąjungos teisę srityje.

4. Ši direktyva taikoma nedarant poveikio Tarybos direktyvai 2008/114/EB[30] ir Europos Parlamento ir Tarybos direktyvoms 2011/93/ES[31] ir 2013/40/ES[32].

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

6. Jeigu pagal konkrečiam sektoriui taikomą Sąjungos teisės aktą reikalaujama, kad esminiai arba svarbūs subjektai priimtų kibernetinio saugumo rizikos valdymo priemones arba praneštų apie incidentus arba dideles kibernetines grėsmes, ir jeigu tie reikalavimai iš esmės yra bent jau lygiaverčiai šioje direktyvoje nustatytoms pareigoms, atitinkamos šios direktyvos nuostatos, įskaitant VI skyriaus nuostatą dėl priežiūros ir vykdymo užtikrinimo, netaikomos.

3 straipsnis

Būtinas suderinimas

Nedarant poveikio valstybių narių pareigoms pagal Sąjungos teisę, valstybės narės gali pagal šią direktyvą priimti ir išlaikyti nuostatas, kuriomis užtikrinamas aukštesnio lygio kibernetinis saugumas.

4 straipsnis

Apibrėžtys

---

29 *[įrašyti visą pavadinimą ir OL paskelbimo nuorodą, kai ji bus žinoma]*

30 2008 m. gruodžio 8 d. Tarybos direktyva 2008/114/EB dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo (OL L 345, 2008 12 23, p. 75).

31 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).

32 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).

Šioje direktyvoje vartojamų terminų apibrėžtys:

1) tinklų ir informacinė sistema – tai:

   a) elektroninių ryšių tinklas, kaip apibrėžta Direktyvos (ES) 2018/1972 2 straipsnio 1 dalyje;

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

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

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

3) kibernetinis saugumas – kibernetinis augumas, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2019/881[33] 2 straipsnio 1 dalyje;

4) nacionalinė kibernetinio saugumo strategija – nuosekli valstybės narės sistema, kurioje nustatyti tos valstybės narės tinklų ir informacinių sistemų saugumo strateginiai tikslai ir prioritetai;

5) incidentas – bet koks įvykis, kuriuo pažeidžiamas saugomų, perduodamų arba tvarkomų duomenų arba susijusių paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas prieinamumas, autentiškumas, vientisumas arba konfidencialumas;

6) incidento valdymas – visi veiksmai ir procedūros, kuriais siekiama nustatyti, išanalizuoti ir sustabdyti incidentą ir į jį reaguoti;

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

8) pažeidžiamumas – turto, sistemos, proceso ar kontrolės priemonės silpnoji vieta, jautrumas ar trūkumas, kuriais gali būti pasinaudota kibernetinei grėsmei kelti;

9) atstovas – bet koks Sąjungoje įsisteigęs fizinis arba juridinis asmuo, paskirtas veikti tik i) DNS paslaugų teikėjo, aukščiausio lygio domenų (TLD) vardų registro, debesijos kompiuterijos paslaugų teikėjo, duomenų centro paslaugų teikėjo, turinio pristatymo tinklo paslaugų teikėjo, kaip apibrėžta I priedo 8 punkte, arba ii) II priedo 6 punkte nurodytų subjektų, kurie nėra įsisteigę Sąjungoje, vardu, į kurį vietoj subjekto dėl to subjekto pareigų pagal šią direktyvą gali kreiptis nacionalinė kompetentinga institucija arba CSIRT;

10) standartas – standartas, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) Nr. 1025/2012[34] 2 straipsnio 1 dalyje;

---

[33] 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).

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

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

13) domenų vardų sistema (DNS) – hierarchiškai paskirstyta vardų sistema, kuri sudaro sąlygas galutiniams naudotojams gauti paslaugas ir pasinaudoti interneto ištekliais;

14) DNS paslaugų teikėjas – subjektas, kuris galutiniams interneto naudotojams ir kitiems DNS paslaugų teikėjams teikia rekursinio arba patikimo domenų vardų keitimo paslaugas;

15) 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 aukščiausio lygio domeno veikimą, įskaitant jo vardų serverių veikimą, duomenų bazių techninę priežiūrą ir aukščiausio lygio domeno zonos rinkmenų paskirstymą tarp vardų serverių;

16) skaitmeninė paslauga – paslauga, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2015/1535[35] 1 straipsnio 1 dalies b punkte;

17) elektroninė prekyvietė – skaitmeninė paslauga, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2005/29/EB[36] 2 straipsnio n punkte;

18) paieškos sistema – skaitmeninė paslauga, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2019/1150[37] 2 straipsnio 5 dalyje;

19) 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;

20) duomenų centro paslauga – paslauga, kuri apima struktūras arba struktūrų grupes, skirtas informacinių technologijų ir tinklo įrangos centralizuotam pritaikymui, tarpusavio junglumui ir eksploatavimui, teikiant duomenų saugojimo, tvarkymo ir

---

34 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, 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).

35 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).

36 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).

37 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).

transportavimo paslaugas kartu su visa energijos paskirstymo ir aplinkos kontrolės įranga ir infrastruktūra;

21) 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;

22) 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;

23) viešojo administravimo subjektas – bet kuris valstybės narės subjektas, kuris atitinka šiuos kriterijus:

(a) yra įsteigtas siekiant tikslo – tenkinti visuotinės svarbos poreikius, kurie nėra pramoninio ar komercinio pobūdžio;

(b) yra juridinis asmuo;

(c) didžiąja dalimi finansuojamas valstybės, regioninės institucijos arba kitų viešosios teisės reguliuojamų įstaigų, arba jo valdymas yra prižiūrimas tų institucijų ar įstaigų, 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 atsižvelgiant į tarpvalstybinį asmenų, prekių, paslaugų ar kapitalo judėjimą.

Į šią sąvoką neįtraukiami viešojo administravimo subjektai, kurie vykdo veiklą viešojo saugumo, teisėsaugos, gynybos arba nacionalinio saugumo srityse;

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

25) esminis subjektas – bet kurios rūšies subjektas, kuris I priede nurodytas kaip esminis subjektas;

26) svarbus subjektas – bet kurios rūšies subjektas, kuris II priede nurodytas kaip svarbus subjektas.

II SKYRIUS

Koordinuotos kibernetinio reguliavimo sistemos

5 straipsnis
Nacionalinė kibernetinio saugumo strategija

1. Kiekviena valstybė narė priima nacionalinę kibernetinio saugumo strategiją, kurioje apibrėžiami strateginiai tikslai ir tinkamos politikos bei reguliavimo priemonės, kad būtų pasiektas ir išlaikytas aukšto lygmens kibernetinis saugumas. Nacionalinėje kibernetinio saugumo strategijoje visų pirma pateikiama:

(a) valstybių narių kibernetinio saugumo strategijos tikslų ir prioritetų apibrėžtis;

(b) valdymo sistema, kad būtų pasiekti tie tikslai ir įgyvendinti prioritetai, įskaitant 2 dalyje nurodytą politiką ir viešųjų įstaigų ir subjektų, taip pat kitų susijusių subjektų vaidmenis ir pareigas;

(c) vertinimas, atliktas siekiant nustatyti atitinkamus objektus ir kibernetinio saugumo riziką toje valstybėje narėje;

(d) parengties, reagavimo į incidentus ir atkūrimo priemonių, įskaitant viešojo ir privačiojo sektorių bendradarbiavimą, nustatymas;

(e) įvairių institucijų ir dalyvių, dalyvaujančių įgyvendinant nacionalinę kibernetinio saugumo strategiją, sąrašas;

(f) politikos sistema, padedanti užtikrinti geresnį kompetentingų institucijų pagal šią direktyvą ir Europos Parlamento ir Tarybos direktyvą (ES) XXXX/XXXX[38] [Ypatingos svarbos infrastruktūros objektų apsaugos direktyva] koordinavimą siekiant dalytis informacija apie incidentus bei kibernetines grėsmes ir vykdyti priežiūros užduotis.

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

a) politiką dėl kibernetinio saugumo klausimų IRT produktų ir paslaugų, kuriuos esminiai ir svarbūs subjektai naudoja teikdami savo paslaugas, tiekimo grandinėje;

b) gaires dėl su kibernetiniu saugumu susijusių reikalavimų, taikomų IRT produktams ir paslaugoms viešuosiuose pirkimuose, ir tokių reikalavimų specifikacijų;

c) suderinto pažeidžiamumų atskleidimo, kaip apibrėžta 6 straipsnyje, skatinimo ir palengvinimo politiką;

d) politiką, susijusią su bendru atvirojo interneto viešojo pagrindo prieinamumu ir vientisumu;

e) politiką dėl kibernetinio saugumo įgūdžių skatinimo, informuotumo didinimo ir mokslinių tyrimų ir technologinės plėtros iniciatyvų;

f) politiką dėl akademinių ir mokslinių tyrimų institucijų rėmimo siekiant tobulinti kibernetinio saugumo priemones ir saugią tinklų infrastruktūrą;

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

h) politiką, kuria sprendžiami konkretūs MVĮ, visų pirma į šios direktyvos taikymo sritį nepatenkančių MVĮ, poreikiai, ir pateikiamos gairės bei parama joms gerinant savo atsparumą kibernetinio saugumo grėsmėms.

3. Valstybės narės per tris mėnesius nuo savo nacionalinių kibernetinio saugumo strategijų priėmimo apie jas informuoja Komisiją. Valstybės narės pranešime gali nenurodyti konkrečios informacijos, jeigu tai yra griežtai būtina siekiant apsaugoti nacionalinį saugumą.

4. Valstybės narės, remdamosi pagrindiniais veiklos rezultatų rodikliais, vertina savo nacionalines kibernetinio saugumo strategijas ne rečiau kaip kas ketverius metus ir

[38] *[įrašyti visą pavadinimą ir OL paskelbimo nuorodą, kai ji bus žinoma]*

prireikus jas pakeičia. Europos Sąjungos kibernetinio saugumo agentūra (ENISA) valstybėms narėms paprašius padeda joms parengti nacionalinę strategiją ir pagrindinius veiklos rezultatų rodiklius, kuriais remiantis įvertinama strategija.

6 straipsnis

Suderintas pažeidžiamumų atskleidimas ir Europos pažeidžiamumų registras

1. Kiekviena valstybė narė paskiria vieną iš savo CSIRT, kaip nurodyta 9 straipsnyje, koordinuoti suderintą pažeidžiamumų atskleidimą. Paskirta CSIRT veikia kaip patikimas tarpininkas, prireikus lengvinantis sąveiką tarp pranešimą teikiančio subjekto ir gamintojo arba IRT produktų ar IRT paslaugų teikėjo. Jeigu pažeidžiamumas, apie kurį pranešta, yra susijęs su įvairiais IRT produktų gamintojais arba IRT paslaugų teikėjais visoje Sąjungoje, kiekvienos valstybės narės atitinkama paskirtoji CSIRT bendradarbiauja su CSIRT tinklu.
2. ENISA sukuria ir tvarko Europos pažeidžiamumų registrą. Tuo tikslu ENISA sukuria ir prižiūri tinkamas informacines sistemas, politiką ir procedūras, visų pirma siekdama sudaryti sąlygas svarbiems ir esminiams subjektams bei jų tinklų ir informacinių sistemų tiekėjams atskleisti ir registruoti IRT produktų ar paslaugų pažeidžiamumus, taip pat visoms suinteresuotosioms šalims suteikti prieigą prie registre pateiktos informacijos apie pažeidžiamumus. Registre visų pirma pateikiama informacija, kuria apibūdinamas pažeidžiamumas, paveikti IRT produktai ar paslaugos ir pažeidžiamumo rimtumas, atsižvelgiant į aplinkybes, kuriomis jie gali būti naudojami, susijusių pataisų prieinamumą ir, jei jų nėra, pažeidžiamų produktų ir paslaugų naudotojams skirtas gaires, kaip galima sumažinti dėl atskleistų pažeidžiamumų kylančią riziką.

7 straipsnis

Nacionalinės kibernetinio saugumo krizės valdymo sistemos

1. Kiekviena valstybė narė paskiria vieną arba daugiau kompetentingų institucijų, kurios atsako už didelio masto incidentų ir krizių valdymą. Valstybės narės užtikrina, kad kompetentingos institucijos turėtų pakankamai išteklių, reikalingų veiksmingam ir efektyviam joms pavestų užduočių vykdymui.
2. Kiekviena valstybė narė, taikydama šią direktyvą, nustato pajėgumus, objektus ir procedūras, kuriais galima pasinaudoti krizės atveju.
3. Kiekviena valstybė narė priima nacionalinį reagavimo į kibernetinio saugumo incidentus ir krizę planą, kuriame išdėstomi didelio masto kibernetinio saugumo incidentų ir krizių valdymo tikslai ir būdai. Plane visų pirma nustatomi:
   a) nacionalinių pasirengimo priemonių ir veiksmų tikslai;
   b) nacionalinių kompetentingų institucijų užduotys ir pareigos;
   c) krizių valdymo procedūros ir keitimosi informacija kanalai;
   d) pasirengimo priemonės, įskaitant pratybas ir mokymo veiklą;
   e) atitinkamos viešosios ir privačiosios suinteresuotosios šalys 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.

4. Valstybės narės praneša Komisijai apie savo kompetentingų institucijų paskyrimą, nurodytą 1 dalyje, ir pateikia savo nacionalinius reagavimo į kibernetinio saugumo incidentus ir krizes planus, kaip nurodyta 3 dalyje, per tris mėnesius nuo tokio paskyrimo ir tų planų priėmimo. Valstybės narės plane gali nenurodyti konkrečios informacijos, jeigu tai yra griežtai būtina jų nacionaliniam saugumui.

8 straipsnis

Nacionalinės kompetentingos institucijos ir bendrieji informaciniai centrai

1. Kiekviena valstybė narė paskiria vieną arba daugiau kompetentingų institucijų, atsakingų už kibernetinį saugumą ir šios direktyvos VI skyriuje nustatytų priežiūros užduočių vykdymą. Valstybės narės šiuo tikslu gali paskirti jau veikiančią instituciją arba institucijas.

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

3. Kiekviena valstybė narė paskiria vieną nacionalinį bendrąjį kibernetinio saugumo informacinį centrą (toliau – bendrasis informacinis centras). Kai valstybė narė paskiria tik vieną kompetentingą instituciją, ta kompetentinga institucija taip pat vykdo tos valstybės narės bendrojo informacinio centro funkcijas.

4. Kiekvienas bendrasis informacinis centras vykdo ryšių palaikymo funkciją, kad būtų užtikrintas jo valstybės narės institucijų tarpvalstybinis bendradarbiavimas su atitinkamomis kitų valstybių narių institucijomis ir tarpsektorinis bendradarbiavimas su kitomis nacionalinėmis kompetentingomis institucijomis valstybėje narėje.

5. Valstybės narės užtikrina, kad 1 dalyje nurodytos kompetentingos institucijos ir bendri informaciniai centrai turėtų tinkamų išteklių, kad veiksmingai ir efektyviai vykdytų jiems pavestas užduotis ir taip įgyvendintų šios direktyvos tikslus. Valstybės narės užtikrina veiksmingą, efektyvų ir saugų į 12 straipsnyje nurodytą Bendradarbiavimo grupę paskirtų atstovų bendradarbiavimą.

6. Kiekviena valstybė narė nepagrįstai nedelsdama praneša Komisijai apie 1 dalyje nurodytą paskirtą kompetentingą instituciją ir 3 dalyje nurodytą bendrąjį informacinį centrą, jų užduotis ir bet kokius vėlesnius jų pakeitimus. Kiekviena valstybė narė apie paskyrimą skelbia viešai. Komisija paskelbia paskirtų bendrųjų informacinių centrų sąrašą.

9 straipsnis

Reagavimo į kompiuterių saugumo incidentus tarnybos (CSIRT)

1. Kiekviena valstybė narė paskiria vieną arba daugiau CSIRT, kurios laikosi 10 straipsnio 1 dalyje išdėstytų reikalavimų, taikomų bent jau I ir II prieduose nurodytiems sektoriams, pasektoriams arba subjektams, ir kurios atsako už incidentų valdymą pagal aiškiai apibrėžtą procesą. CSIRT gali būti įsteigta kompetentingoje institucijoje, kuri nurodyta 8 straipsnyje.

2. Valstybės narės užtikrina, kad kiekviena CSIRT turėtų tinkamų išteklių, kad galėtų veiksmingai vykdyti savo užduotis, nurodytas 10 straipsnio 2 dalyje.

3. Valstybės narės užtikrina, kad kiekviena CSIRT turėtų tinkamą, saugią ir atsparią ryšių ir informacinę struktūrą, kad galėtų keistis informacija su esminiais ir svarbiais subjektais ir kitomis atitinkamomis suinteresuotosiomis šalimis. Šiuo tikslu valstybės narės užtikrina, kad CSIRT prisidėtų prie saugaus dalijimosi informacija priemonių diegimo.

4. CSIRT pagal 26 straipsnį bendradarbiauja ir, kai tinkama, keičiasi atitinkama informacija su patikimomis sektoriaus arba kelių sektorių esminių ir svarbių subjektų bendruomenėmis.

5. CSIRT dalyvauja tarpusavio vertinimuose, kurie atliekami pagal 16 straipsnį.

6. Valstybės narės užtikrina efektyvų, veiksmingą ir saugų jų CSIRT bendradarbiavimą 13 straipsnyje nurodytame CSIRT tinkle.

7. Valstybės narės nepagrįstai nedelsdamos praneša Komisijai apie pagal 1 dalį paskirtas CSIRT, CSIRT koordinatorių, paskirtą pagal 6 straipsnio 1 dalį, ir jų atitinkamas užduotis, kurias jos vykdo I ir II prieduose išvardytų subjektų atžvilgiu.

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

10 straipsnis
CSIRT keliami reikalavimai ir užduotys

1. CSIRT turi atitikti šiuos reikalavimus:

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

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

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

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

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

   f) CSIRT turi galimybę dalyvauti tarptautiniuose bendradarbiavimo tinkluose.

2. CSIRT vykdo šias užduotis:

   a) stebi kibernetines grėsmes, pažeidžiamumus ir incidentus nacionaliniu lygmeniu;

   b) teikia išankstinius įspėjimus, perspėjimus, pranešimus ir platina informaciją apie kibernetines grėsmes, pažeidžiamumus ir incidentus esminiams ir svarbiems subjektams, taip pat kitoms atitinkamoms suinteresuotosioms šalims;

   c) reaguoja į incidentus;

d) užtikrina operatyvią rizikos bei incidentų analizę ir informuotumą apie kibernetinio saugumo padėtį;

e) subjekto prašymu aktyviai patikrina tinklų ir informacines sistemas, kurias subjektas naudoja teikdamas paslaugas;

f) dalyvauja CSIRT tinkle ir teikia savitarpio pagalbą kitiems tinklo nariams jų prašymu.

3. CSIRT užmezga bendradarbiavimo ryšius su atitinkamais privačiojo sektoriaus subjektais, kad būtų geriau pasiekti direktyvos tikslai.

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

a) incidentų valdymo procedūromis;

b) kibernetinio saugumo krizės valdymu;

c) suderintu pažeidžiamumų atskleidimu.

11 straipsnis

Bendradarbiavimas nacionaliniu lygmeniu

1. Kai tos pačios valstybės narės kompetentingos institucijos, nurodytos 8 straipsnyje, bendrasis informacinis centras ir CSIRT yra atskiri, jie bendradarbiauja tarpusavyje, kad vykdytų šioje direktyvoje nustatytas pareigas.

2. Valstybės narės užtikrina, kad jų kompetentingos institucijos arba CSIRT gautų šioje direktyvoje nustatyta tvarka pateikiamus pranešimus apie incidentus, dideles kibernetines grėsmes ir vos neįvykusius incidentus. Jeigu valstybė narė nusprendžia, kad jos CSIRT neturi gauti pranešimų, CSIRT, kiek tai būtina jų užduotims vykdyti, suteikiama prieiga prie duomenų apie incidentus, apie kuriuos pranešė esminiai ar svarbūs subjektai pagal 20 straipsnį.

3. Kiekviena valstybė narė užtikrina, kad jos kompetentingos institucijos arba CSIRT informuotų savo bendrąjį informacinį centrą apie šioje direktyvoje nustatyta tvarka pateikiamus pranešimus apie incidentus, dideles kibernetines grėsmes ir vos neįvykusius incidentus.

4. Tiek, kiek būtina tam, kad šioje direktyvoje nustatytos užduotys ir pareigos būtų vykdomos veiksmingai, valstybės narės užtikrina tinkamą kompetentingų institucijų ir bendrųjų informacinių centrų, teisėsaugos institucijų, duomenų apsaugos institucijų ir institucijų, atsakingų už ypatingos svarbos infrastruktūros objektus pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva] ir nacionalinių finansų institucijų, paskirtų pagal Europos Parlamento ir Tarybos reglamentą (ES) XXXX/XXXX[39] [DORA reglamentas], bendradarbiavimą toje valstybėje narėje.

5. Valstybės narės užtikrina, kad jų kompetentingos institucijos reguliariai teiktų informaciją pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva] paskirtoms kompetentingoms institucijoms apie kibernetinio

[39] *[įrašyti visą pavadinimą ir OL paskelbimo nuorodą, kai ji bus žinoma]*

saugumo riziką, kibernetines grėsmes ir incidentus, darančius poveikį esminiams subjektams, kurie pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva] laikomi ypatingos svarbos subjektais arba ypatingos svarbos subjektams lygiaverčiais subjektais, taip pat apie priemones, kurių kompetentingos institucijos ėmėsi reaguodamos į tą riziką ir incidentus.

III SKYRIUS

Bendradarbiavimas

12 straipsnis
Bendradarbiavimo grupė

1. Siekiant remti ir palengvinti strateginį bendradarbiavimą ir keitimąsi informacija tarp valstybių narių direktyvos taikymo srityje, sudaroma Bendradarbiavimo grupė.

2. Bendradarbiavimo grupė vykdo savo užduotis remdamasi dvimetėmis darbo programomis, nurodytomis 6 dalyje.

3. Bendradarbiavimo grupę sudaro valstybių narių, Komisijos ir ENISA atstovai. Europos išorės veiksmų tarnyba Bendradarbiavimo grupėje dalyvauja stebėtojos teisėmis. Europos priežiūros institucijos (EPI) pagal Reglamento (ES) XXXX/XXXX [DORA reglamentas] 17 straipsnio 5 dalies c punktą gali dalyvauti Bendradarbiavimo grupės veikloje.

   Prireikus Bendradarbiavimo grupė gali pakviesti atitinkamų suinteresuotųjų šalių 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) 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, taip pat standartais ir techninėmis specifikacijomis;

   c) keičiasi patarimais ir bendradarbiauja su Komisija dėl naujų kibernetinio saugumo politikos iniciatyvų;

   d) keičiasi patarimais ir bendradarbiauja su Komisija dėl Komisijos įgyvendinimo arba deleguotųjų aktų, priimtų pagal šią direktyvą, projektų;

   e) keičiasi geriausia patirtimi ir informacija su atitinkamomis Sąjungos institucijomis, įstaigomis, biurais ir agentūromis;

   f) aptaria 16 straipsnio 7 dalyje nurodytas tarpusavio vertinimo ataskaitas;

g) aptaria bendros priežiūros veiklos tarpvalstybiniais atvejais, kaip nurodyta 34 straipsnyje, rezultatus;

h) teikia strategines gaires CSIRT tinklui konkrečiais kylančiais klausimais;

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

j) organizuoja nuolatinius bendrus susitikimus su atitinkamomis privačiomis suinteresuotosiomis šalimis iš visos Sąjungos, kad aptartų grupės vykdomą veiklą ir surinktų informacijos apie naujus politikos uždavinius;

k) aptaria su kibernetinio saugumo pratybomis susijusį darbą, įskaitant ENISA atliktą darbą.

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

6. Iki… [24 mėnesiai po šios direktyvos įsigaliojimo dienos], o vėliau kas dvejus metus Bendradarbiavimo grupė parengia darbo programą, skirtą veiksmams, kurių reikia imtis jos tikslams ir uždaviniams įgyvendinti. Pirmosios pagal šią direktyvą priimtos programos laikotarpis yra suderinamas su paskutinės programos, priimtos pagal Direktyvą (EU) 2016/1148, laikotarpiu.

7. Komisija gali priimti įgyvendinimo aktus, kuriais nustatoma procedūrinė tvarka, būtina Bendradarbiavimo grupės veikimui užtikrinti. Tie įgyvendinimo aktai priimami laikantis 37 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

8. Bendradarbiavimo grupė nuolat ir ne rečiau kaip kartą per metus susitinka su Ypatingos svarbos subjektų atsparumo klausimų grupe, sudaryta pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva], kad skatintų strateginį bendradarbiavimą ir keitimąsi informacija.

13 straipsnis
CSIRT tinklas

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

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

3. CSIRT tinklas vykdo šias užduotis:

(a) keičiasi informacija apie CSIRT pajėgumus;

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

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

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

(e) teikia valstybėms narėms paramą šalinant tarpvalstybinius incidentus pagal šią direktyvą;

(f) bendradarbiauja ir teikia paramą pagal 6 straipsnį paskirtosioms CSIRT, susijusią su įvairių šalių suderintu pažeidžiamumų, darančių poveikį įvairiems IRT produktų, IRT paslaugų ir IRT procesų gamintojams ir teikėjams, kurie yra įsisteigę įvairiose valstybėse narėse, atskleidimo valdymu;

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

i) kibernetinių grėsmių ir incidentų kategorijomis;

ii) išankstiniais įspėjimais;

iii) savitarpio pagalba;

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

v) pagalba rengiant nacionalinį reagavimo į kibernetinio saugumo incidentus ir krizes planą, nurodytą 7 straipsnio 3 dalyje;

(h) informuoja Bendradarbiavimo grupę apie savo veiklą ir tolesnes operatyvinio bendradarbiavimo formas, aptartas pagal g punktą, ir prireikus prašo šiuo atžvilgiu pateikti rekomendacijų;

(i) naudojasi kibernetinio saugumo pratybomis, įskaitant ENISA organizuojamas pratybas;

(j) atskiros CSIRT prašymu aptaria tos CSIRT pajėgumus ir parengtį;

(k) 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;

(l) aptaria 16 straipsnio 7 dalyje nurodytas tarpusavio vertinimo ataskaitas;

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

4. Atsižvelgiant į 35 straipsnyje nurodytą peržiūrą, ne vėliau kaip iki [24 mėnesiai nuo šios direktyvos įsigaliojimo datos] ir paskui kas dvejus metus CSIRT tinklas įvertina padarytą pažangą operatyvinio bendradarbiavimo srityje ir parengia ataskaitą. Ataskaitoje visų pirma pateikiamos išvados dėl 16 straipsnyje nurodytų tarpusavio vertinimų, atliktų dėl šiame straipsnyje nurodytų nacionalinių CSIRT, rezultatų, įskaitant išvadas ir rekomendacijas. Ta ataskaita taip pat pateikiama Bendradarbiavimo grupei.

5. CSIRT tinklas priima savo darbo tvarkos taisykles.

14 straipsnis

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

1. Siekiant remti koordinuotą didelio masto kibernetinio saugumo incidentų ir krizių valdymą veiklos lygmeniu ir užtikrinti reguliarų keitimąsi informacija tarp valstybių narių ir Sąjungos institucijų, įstaigų ir agentūrų, įsteigiamas Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas („EU-CyCLONe“).

2. „EU-CyCLONe“ sudaro valstybių narių krizių valdymo institucijų, paskirtų pagal 7 straipsnį, Komisijos ir ENISA atstovai. ENISA teikia tinklo sekretoriato paslaugas ir padeda saugiai keistis informacija.

3. „EU-CyCLONe“ vykdo šias užduotis:

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

   b) plėtoja bendrą informuotumą apie padėtį, susijusią su atitinkamais kibernetinio saugumo įvykiais;

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

   d) aptaria 7 straipsnio 2 dalyje nurodytus nacionalinius reagavimo į kibernetinio saugumo incidentus ir krizes planus.

4. „EU-CyCLONe“ priima savo darbo tvarkos taisykles.

5. „EU-CyCLONe“ reguliariai informuoja Bendradarbiavimo grupę apie kibernetines grėsmes, incidentus ir tendencijas, ypatingą dėmesį skirdamas jų poveikiui esminiams ir svarbiems subjektams.

6. „EU-CyCLONe“ su CSIRT tinklu bendradarbiauja remdamasis sutartomis procedūrinėmis taisyklėmis.

15 straipsnis

Kibernetinio saugumo būklės Sąjungoje ataskaita

1. ENISA, bendradarbiaudama su Komisija, kas dvejus metus rengia kibernetinio saugumo Sąjungoje būklės ataskaitą. Ataskaitoje visų pirma įvertinami šie aspektai:

   (a) kibernetinio saugumo pajėgumų Sąjungoje plėtojimas;

   (b) kompetentingų institucijų turimi techniniai, finansiniai ir žmogiškieji ištekliai ir kibernetinio saugumo politika, taip pat priežiūros priemonių ir vykdymo užtikrinimo veiksmų įgyvendinimas atsižvelgiant į 16 straipsnyje nurodytų tarpusavio vertinimų rezultatus;

   (c) kibernetinio saugumo indeksas, kuriame atsispindi apibendrintas kibernetinio saugumo pajėgumų brandos vertinimas.

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

16 straipsnis

Tarpusavio vertinimai

1. Komisija, pasikonsultavusi su Bendradarbiavimo grupe ir ENISA, ir ne vėliau kaip per 18 mėnesių nuo šios direktyvos įsigaliojimo nustato tarpusavio vertinimo sistemos, skirtos valstybių narių kibernetinio saugumo politikos veiksmingumui įvertinti, metodiką ir turinį. Peržiūras atlieka kibernetinio saugumo techniniai ekspertai, atrinkti iš valstybių narių, kuriose peržiūra neatlikta, ir jos apima bent šiuos aspektus:

   i) kibernetinio saugumo rizikos valdymo reikalavimų ir pranešimo pareigų, nurodytų 18 ir 20 straipsniuose, įgyvendinimo veiksmingumą;

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

   iii) CSIRT operatyvinius pajėgumus ir veiksmingumą;

   iv) 34 straipsnyje nurodytos savitarpio pagalbos veiksmingumą;

   v) šios direktyvos 26 straipsnyje nurodytos keitimosi informacija sistemos veiksmingumą.

2. Metodika apima objektyvius, nediskriminacinius, sąžiningus ir skaidrius kriterijus, kuriais remdamosi valstybės narės paskiria ekspertus, atitinkančius reikalavimus tarpusavio vertinimui atlikti. ENISA ir Komisija paskiria ekspertus dalyvauti tarpusavio vertinimuose stebėtojų teisėmis. Komisija, padedama ENISA, pagal 1 dalyje nurodytą metodiką nustato objektyvią, nediskriminacinę, sąžiningą ir skaidrią kiekvieno tarpusavio vertinimo ekspertų atrankos ir atsitiktinio paskyrimo sistemą.

3. Dėl tarpusavio vertinimų organizacinių aspektų sprendžia Komisija, padedama ENISA, ir, pasikonsultavus su Bendradarbiavimo grupe, jie grindžiami kriterijais, apibrėžtais 1 dalyje nurodytoje metodikoje. Atliekant tarpusavio vertinimus įvertinami 1 dalyje nurodyti visų valstybių narių ir sektorių aspektai, įskaitant tikslinius vienai ar kelioms valstybėms narėms arba vienam ar keliems sektoriams būdingus klausimus.

4. Tarpusavio vertinimai apima faktinius arba virtualius apsilankymus vietoje ir keitimąsi informacija ne vietoje. Atsižvelgiant į gero bendradarbiavimo principą, valstybės narės, kuriose atliekama peržiūra, pateikia paskirtiems ekspertams prašomą informaciją, reikalingą peržiūrėtiems aspektams įvertinti. Visa per tarpusavio vertinimą gauta informacija naudojama tik tam vertinimui. Tarpusavio vertinime dalyvaujantys ekspertai neatskleidžia jokios per tą peržiūrą gautos neskelbtinos ar konfidencialios informacijos jokioms trečiosioms šalims.

5. Valstybėje narėje tie patys peržiūrėti aspektai dvejus metus po tarpusavio vertinimo pabaigos toje valstybėje narėje toliau netikrinami, nebent Komisija, pasikonsultavusi su ENISA ir Bendradarbiavimo grupe, nuspręstų kitaip.

6. Valstybė narė užtikrina, kad bet kokia su paskirtais ekspertais susijusi interesų konflikto rizika būtų nepagrįstai nedelsiant atskleista kitoms valstybėms narėms, Komisijai ir ENISA.

7. Tarpusavio vertinimuose dalyvaujantys ekspertai parengia per peržiūras nustatytų faktų ir išvadų ataskaitas. Ataskaitos teikiamos Komisijai, Bendradarbiavimo grupei, CSIRT tinklui ir ENISA. Ataskaitos aptariamos Bendradarbiavimo grupėje ir CSIRT tinkle. Ataskaitos gali būti skelbiamos Bendradarbiavimo grupės interneto svetainėje.

IV SKYRIUS

Kibernetinio saugumo rizikos valdymas ir pareigos pranešti

I SKIRSNIS

Kibernetinio saugumo rizikos valdymas ir pranešimų teikimas

17 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 18 straipsnio, prižiūrėti jų įgyvendinimą ir būti atskaitingi už tai, kad subjektai nesilaiko šiame straipsnyje nustatytų pareigų.

2. Valstybės narės užtikrina, kad valdymo organo nariai reguliariai dalyvautų specialiuose mokymuose, kad įgytų pakankamai žinių ir įgūdžių, kad galėtų suprasti ir įvertinti kibernetinio saugumo riziką ir valdymo praktiką bei jos poveikį subjekto veiklai.

18 straipsnis

Kibernetinio saugumo rizikos valdymo priemonės

1. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai imtųsi tinkamų ir proporcingų techninių ir organizacinių priemonių, siekdami valdyti tinklų ir informacinių sistemų, kurias tie subjektai naudoja teikdami savo paslaugas, saugumui kylančią riziką. Remiantis naujausiais technikos laimėjimais, tomis priemonėmis turi būti užtikrinamas toks tinklų ir informacinių sistemų saugumo lygis, kuris atitinka kylančią riziką.

2. 1 dalyje nurodytos priemonės apima bent:

   (a) rizikos analizę ir informacinių sistemų saugumo politiką;

   (b) incidentų valdymą (incidentų prevencija, aptikimas ir reagavimas į juos);

   (c) veiklos tęstinumą ir krizių valdymą;

   (d) tiekimo grandinės saugumą, įskaitant su saugumu susijusius aspektus, susijusius su kiekvieno subjekto ir jo tiekėjų ar paslaugų teikėjų, pavyzdžiui, duomenų saugojimo ir tvarkymo paslaugų teikėjų arba valdomų saugumo paslaugų teikėjų, santykiais;

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

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

   (g) kriptografijos ir šifravimo naudojimą.

3. Valstybės narės užtikrina, kad, svarstydami 2 dalies d punkte nurodytas tinkamas priemones, subjektai atsižvelgtų į kiekvieno tiekėjo ir paslaugų teikėjo pažeidžiamumą ir į jų tiekėjų ir paslaugų teikėjų produktų bendrą kokybę ir kibernetinio saugumo praktiką, įskaitant jų saugumo plėtojimo procedūras.

4. Valstybės narės užtikrina, kad tais atvejais, kai subjektas nustato, kad atitinkamai jo paslaugos ar užduotys neatitinka 2 dalyje nustatytų reikalavimų, jis nepagrįstai nedelsdamas imtųsi visų būtinų taisomųjų priemonių, kad atitinkama paslauga atitiktų reikalavimus.

5. Komisija gali priimti įgyvendinimo aktus, kuriais nustatomos 2 dalyje nurodytų aspektų techninės ir metodinės specifikacijos. Rengdama tuos aktus Komisija laikosi 37 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros ir, kiek įmanoma, laikosi tarptautinių ir Europos standartų bei atitinkamų techninių specifikacijų.

6. Siekiant atsižvelgti į naujas kibernetines grėsmes, technologinę plėtrą ar sektorių ypatumus, Komisijai pagal 36 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, kuriais papildomi 2 dalyje nustatyti aspektai.

19 straipsnis

ES suderinti ypatingos svarbos tiekimo grandinių rizikos vertinimai

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

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

20 straipsnis

Pareigos pranešti

1. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai nepagrįstai nedelsdami praneštų kompetentingoms institucijoms arba CSIRT pagal 3 ir 4 dalis apie bet kokį incidentą, turintį didelį poveikį jų paslaugų teikimui. Kai tinkama, tie subjektai nepagrįstai nedelsdami praneša jų paslaugų gavėjams apie incidentus, kurie gali turėti neigiamos įtakos tos paslaugos teikimui. Valstybės narės užtikrina, kad tie subjektai, be kita ko, praneštų visą informaciją, pagal kurią kompetentingos institucijos arba CSIRT galėtų nustatyti tarpvalstybinį incidento poveikį.

2. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai nepagrįstai nedelsdami praneštų kompetentingoms institucijoms arba CSIRT apie bet kokią didelę kibernetinę grėsmę, kurią tie subjektai nustatė ir dėl kurios galėtų įvykti didelis incidentas.

   Kai taikytina, tie subjektai nepagrįstai nedelsdami praneša savo paslaugų gavėjams, kuriems gali daryti poveikį didelė kibernetinė grėsmė, 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 grėsmę. Dėl pranešimo pranešančiojo subjekto atsakomybė nepadidėja.

3. Incidentas laikomas rimtu, jeigu:

(a) dėl incidento atitinkamas subjektas patyrė arba gali patirti didelių veiklos sutrikimų arba finansinių nuostolių;

(b) incidentas paveikė arba gali paveikti kitus fizinius ar juridinius asmenis dėl didelių materialinių arba neturtinių nuostolių.

4. Valstybės narės užtikrina, kad 1 dalyje nurodyto pranešimo tikslais atitinkami subjektai kompetentingoms institucijoms arba CSIRT pateiktų:

(a) nepagrįstai nedelsiant ir bet kuriuo atveju per 24 valandas nuo to laiko, kai sužinoma apie incidentą, – pradinį pranešimą, kuriame, kai taikoma, nurodoma, ar incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai;

(b) kompetentingos institucijos arba CSIRT prašymu – tarpinę ataskaitą apie atitinkamus atnaujintus duomenis apie padėtį;

(c) ne vėliau kaip per vieną mėnesį nuo a punkte nurodytos ataskaitos pateikimo – galutinę ataskaitą, kurioje pateikiama bent ši informacija:

i) išsamus incidento, jo sunkumo ir poveikio aprašymas;

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

iii) taikomos ir įgyvendinamos poveikio mažinimo priemonės.

Valstybės narės nustato, kad tinkamai pagrįstais atvejais ir susitarus su kompetentingomis institucijomis arba CSIRT atitinkamas subjektas gali nukrypti nuo a ir c punktuose nustatytų terminų.

5. Kompetentingos nacionalinės institucijos arba CSIRT per 24 valandas nuo 4 dalies a punkte nurodyto pirminio pranešimo gavimo pateikia atsakymą pranešimą teikiančiam subjektui, įskaitant pirminę grįžtamąją informaciją apie incidentą, o subjekto prašymu – galimų rizikos mažinimo priemonių įgyvendinimo gaires. Jei CSIRT negavo 1 dalyje nurodyto pranešimo, gaires teikia kompetentinga institucija, bendradarbiaudama su CSIRT. CSIRT teikia papildomą techninę pagalbą, jei to prašo atitinkamas subjektas. Jei įtariama, kad incidentas yra baudžiamojo pobūdžio, kompetentingos nacionalinės institucijos arba CSIRT taip pat teikia gaires dėl pranešimo apie incidentą teisėsaugos institucijoms.

6. Atitinkamais atvejais ir visų pirma tuomet, kai 1 dalyje nurodytas incidentas susijęs su dviem ar daugiau valstybių narių, kompetentinga institucija arba CSIRT apie incidentą informuoja kitas paveiktas valstybes nares ir ENISA. Tai darydamos kompetentingos institucijos, CSIRT ir bendrieji informaciniai centrai pagal Sąjungos teisę arba Sąjungos teisę atitinkančius nacionalinės teisės aktus saugo subjekto saugumo ir komercinius interesus, taip pat pateiktos informacijos konfidencialumą.

7. Kai visuomenės informuotumas yra būtinas siekiant užkirsti kelią incidentui ar reaguoti į besitęsiantį incidentą arba kai incidento atskleidimas kitais atvejais atitinka viešąjį interesą, kompetentinga institucija arba CSIRT ir atitinkamais atvejais kitų atitinkamų valstybių narių institucijos arba CSIRT, pasikonsultavusios su atitinkamu

subjektu, gali informuoti visuomenę apie incidentą arba pareikalauti, kad tai padarytų subjektas.

8. Kompetentingos institucijos arba CSIRT prašymu bendrasis informacinis centras perduoda pagal 1 ir 2 dalis gautus pranešimus kitų paveiktų valstybių narių bendriesiems informaciniams centrams.

9. Bendrasis informacinis centras kas mėnesį teikia ENISA suvestinę ataskaitą, į kurią įtraukiami anoniminiai ir suvestiniai duomenys apie incidentus, dideles kibernetines grėsmes ir vos neįvykusius incidentus, apie kuriuos pranešta pagal 1 ir 2 dalis ir pagal 27 straipsnį. Siekdama prisidėti prie palyginamos informacijos teikimo ENISA gali paskelbti technines gaires dėl į suvestinę ataskaitą įtrauktos informacijos parametrų.

10. Kompetentingos institucijos pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva] paskirtoms kompetentingoms institucijoms teikia informaciją apie incidentus ir kibernetines grėsmes, apie kuriuos pagal 1 ir 2 dalis pranešė esminiai subjektai, nustatyti kaip ypatingos svarbos subjektai arba ypatingos svarbos subjektams lygiaverčiai subjektai, pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva].

11. Komisija gali priimti įgyvendinimo aktus, kuriais išsamiau nustatoma pagal 1 ir 2 dalis pateikto pranešimo rūšis, formatas ir procedūra. Komisija taip pat gali priimti įgyvendinimo aktus, kuriais išsamiau nustatomi atvejai, kuriais incidentas laikomas rimtu, kaip nurodyta 3 dalyje. Tie įgyvendinimo aktai priimami laikantis 37 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

21 straipsnis

Europos kibernetinio saugumo sertifikavimo schemų naudojimas

1. Siekdamos įrodyti atitiktį tam tikriems 18 straipsnio reikalavimams, valstybės narės gali reikalauti, kad esminiai ir svarbūs subjektai sertifikuotų tam tikrus IRT produktus, paslaugas ir procesus pagal konkrečias Europos kibernetinio saugumo sertifikavimo schemas, priimtas pagal Reglamento (ES) 2019/881 49 straipsnį. Sertifikuojamus produktus, paslaugas ir procesus gali kurti esminis arba svarbus subjektas arba jie gali būti perkami iš trečiųjų šalių.

2. Komisijai suteikiami įgaliojimai priimti deleguotuosius aktus, kuriais nustatoma, kokių kategorijų esminiams subjektams reikia gauti sertifikatą ir pagal kurias konkrečias Europos kibernetinio saugumo sertifikavimo schemas pagal 1 dalį. Deleguotieji aktai priimami pagal 36 straipsnį.

3. Komisija gali prašyti ENISA parengti potencialią schemą pagal Reglamento (ES) 2019/881 48 straipsnio 2 dalį tais atvejais, kai nėra tinkamos Europos kibernetinio saugumo sertifikavimo schemos 2 dalies tikslais.

22 straipsnis

Standartizacija

1. Siekdamos skatinti vienodą 18 straipsnio 1 ir 2 dalių įgyvendinimą, valstybės narės, nereikalaudamos taikyti kokios nors konkrečios rūšies technologijos ir

nesuteikdamos jai pirmenybės, skatina naudotis europiniais ar tarptautiniu mastu pripažintais standartais ir specifikacijomis, kurie yra svarbūs tinklų ir informacinių sistemų saugumui.

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

23 straipsnis

Domenų vardų ir registracijos duomenų bazės

1. Siekdamos prisidėti prie DNS saugumo, stabilumo ir atsparumo, valstybės narės užtikrina, kad aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys domenų vardų registravimo paslaugas aukščiausio lygio domenų vardams, su deramu stropumu rinktų ir specialioje duomenų bazėje saugotų tikslius ir išsamius domenų vardų registracijos duomenis, kuriems taikomi Sąjungos duomenų apsaugos teisės aktai dėl duomenų, kurie yra asmens duomenys.

2. Valstybės narės užtikrina, kad 1 dalyje nurodytose domenų vardų registracijos duomenų bazėse būtų atitinkama informacija, pagal kurią būtų galima nustatyti domenų vardų turėtojus ir kontaktinius centrus, administruojančius aukščiausio lygio domenų vardais pažymėtus domenų vardus, ir su jais susisiekti.

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

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

5. Valstybės narės užtikrina, kad aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys domenų vardų registravimo paslaugas aukščiausio lygio domenų vardams, gavę teisėtus ir tinkamai pagrįstus siekiančių gauti prieigą subjektų prašymus, suteiktų prieigą prie konkrečių domenų vardų registracijos duomenų, laikydamiesi Sąjungos duomenų apsaugos teisės aktų. Valstybės narės užtikrina, kad aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys domenų vardų registravimo paslaugas aukščiausio lygio domenų vardams, nepagrįstai nedelsdami atsakytų į visus prašymus suteikti prieigą. Valstybės narės užtikrina, kad tokių duomenų atskleidimo politika ir procedūros būtų skelbiamos viešai.

II skirsnis

Jurisdikcija ir registracija

24 straipsnis

Jurisdikcija ir teritoriškumas

1. DNS paslaugų teikėjai, aukščiausio lygio domenų vardų registrai, debesijos kompiuterijos paslaugų teikėjai, duomenų centrų paslaugų teikėjai ir turinio teikimo tinklo paslaugų teikėjai, nurodyti I priedo 8 punkte, taip pat II priedo 6 punkte nurodyti skaitmeninių paslaugų teikėjai laikomi priklausančiais valstybės narės, kurioje yra jų pagrindinė buveinė Sąjungoje, jurisdikcijai.

2. Taikant šią direktyvą laikoma, kad 1 dalyje nurodytų subjektų pagrindinė buveinė Sąjungoje yra valstybėje narėje, kurioje priimami su kibernetinio saugumo rizikos valdymo priemonėmis susiję sprendimai. Jei tokie sprendimai nepriimami jokiame padalinyje Sąjungoje, laikoma, kad pagrindinė buveinė yra valstybėje narėje, kurioje subjekto padalinyje dirba daugiausia darbuotojų Sąjungoje.

3. Jei 1 dalyje nurodytas subjektas nėra įsisteigęs Sąjungoje, bet teikia paslaugas Sąjungoje, jis paskiria atstovą Sąjungoje. Atstovas turi būti įsisteigęs vienoje iš tų valstybių narių, kuriose teikiamos paslaugos. Laikoma, kad toks subjektas priklauso valstybės narės, kurioje yra įsisteigęs jo atstovas, jurisdikcijai. Jei pagal šį straipsnį Sąjungoje nėra paskirto atstovo, bet kuri valstybė narė, kurioje subjektas teikia paslaugas, gali imtis teisinių veiksmų prieš subjektą dėl šioje direktyvoje nustatytų pareigų nevykdymo.

4. 1 dalyje nurodyto subjekto atstovo paskyrimas nedaro poveikio teisiniams veiksmams, kurie galėtų būti inicijuoti prieš patį subjektą.

25 straipsnis

Esminių ir svarbių subjektų registras

1. ENISA sukuria ir tvarko 24 straipsnio 1 dalyje nurodytų esminių ir svarbių subjektų registrą. Subjektai ne vėliau kaip [12 mėnesių po direktyvos įsigaliojimo] pateikia ENISA šią informaciją:

   (a) subjekto pavadinimą;

   (b) savo pagrindinės buveinės adresą ir kitus juridinius padalinius Sąjungoje arba, jei jie nėra įsisteigę Sąjungoje, pagal 24 straipsnio 3 dalį paskirto atstovo adresą;

   (c) naujausius kontaktinius duomenis, įskaitant subjektų e. pašto adresus ir telefono numerius.

2. 1 dalyje nurodyti subjektai nedelsdami ir bet kuriuo atveju ne vėliau kaip per tris mėnesius nuo pakeitimo įsigaliojimo dienos praneša ENISA apie bet kokius pagal 1 dalį pateiktos informacijos pakeitimus.

3. Gavusi 1 dalyje nurodytą informaciją ENISA perduoda ją bendriesiems informaciniams centrams, atsižvelgdama į nurodytą kiekvieno subjekto pagrindinės buveinės vietą arba, jei ji nėra įsisteigusi Sąjungoje, jos paskirto atstovo vietą. Jei 1 dalyje nurodytas subjektas turi ne tik pagrindinę buveinę Sąjungoje, bet ir kitas buveines kitose valstybėse narėse, ENISA taip pat informuoja tų valstybių narių bendruosius informacinius centrus.

4. Jei subjektas neužregistruoja savo veiklos arba nepateikia atitinkamos informacijos per 1 dalyje nustatytą terminą, bet kuri valstybė narė, kurioje subjektas teikia paslaugas, turi kompetenciją užtikrinti, kad tas subjektas laikytųsi šioje direktyvoje nustatytų pareigų.

V SKYRIUS

Dalijimasis informacija

26 straipsnis

Dalijimosi kibernetinio saugumo informacija taisyklės

1. Nedarant poveikio Reglamentui (ES) 2016/679, valstybės narės užtikrina, kad esminiai ir svarbūs subjektai galėtų tarpusavyje keistis svarbia kibernetinio saugumo informacija, įskaitant informaciją, susijusią su kibernetinėmis grėsmėmis, pažeidžiamumu, užvaldymo rodikliais, taktika, metodais ir procedūromis, kibernetinio saugumo perspėjimais ir konfigūracijos priemonėmis, kai tokiu dalijimusi informacija:

   (a) siekiama užkirsti kelią incidentams, juos nustatyti, į juos reaguoti arba juos sušvelninti;

   (b) didinamas kibernetinis saugumas, visų pirma didinant informuotumą apie kibernetines grėsmes, ribojant arba trukdant tokioms grėsmėms plisti, remiant įvairius gynybos pajėgumus, pažeidžiamumo ištaisymą ir atskleidimą, grėsmių nustatymo metodus, švelninimo strategijas arba reagavimo ir atsigavimo etapus.

2. Valstybės narės užtikrina, kad informacija būtų keičiamasi patikimose esminių ir svarbių subjektų bendruomenėse. Toks keitimasis vykdomas taikant dalijimosi informacija susitarimus, susijusius su galimai neskelbtina informacija, kuria keičiamasi, ir laikantis 1 dalyje nurodytų Sąjungos teisės taisyklių.

3. Valstybės narės nustato taisykles, kuriose aprašoma 2 dalyje nurodytų dalijimosi informacija susitarimų procedūra, veiklos elementai (įskaitant specialių IRT platformų naudojimą), turinys ir sąlygos. Tokiose taisyklėse taip pat nustatoma išsami informacija apie valdžios institucijų dalyvavimą tokiuose susitarimuose, taip pat veiklos elementai, įskaitant specialių IT platformų naudojimą. Valstybės narės teikia paramą tokių priemonių taikymui pagal 5 straipsnio 2 dalies g punkte nurodytą savo politiką.

4. Esminiai ir svarbūs subjektai kompetentingoms institucijoms praneša apie savo dalyvavimą 2 dalyje nurodytuose dalijimosi informacija susitarimuose jiems įsigaliojus arba, kai tinkama, apie pasitraukimą iš tokių susitarimų, kai toks pasitraukimas įsigalioja.

5. Laikydamasi Sąjungos teisės ENISA remia 2 dalyje nurodytų dalijimosi kibernetinio saugumo informacija susitarimų sudarymą, teikdama geriausios praktikos pavyzdžius ir gaires.

27 straipsnis

Savanoriškas pranešimas apie svarbią informaciją

Valstybės narės užtikrina, kad, nedarant poveikio 3 straipsniui, subjektai, kuriems ši direktyva netaikoma, galėtų savanoriškai teikti pranešimus apie didelius incidentus, kibernetines grėsmes arba vos neįvykusius incidentus. Tvarkydamos tokius pranešimus valstybės narės veikia pagal 20 straipsnyje nustatytą procedūrą. Valstybės narės gali teikti pirmenybę privalomų pranešimų tvarkymui, lyginant su savanoriškais pranešimais. Dėl savanoriško pranešimo pranešančiajam subjektui nenustatoma jokių papildomų pareigų, kurios jam nebūtų taikomos, jei jis nebūtų pateikęs pranešimo.

VI SKYRIUS

Priežiūra ir vykdymo užtikrinimas

28 straipsnis

Bendrieji aspektai, susiję su priežiūra ir vykdymo užtikrinimu

1. Valstybės narės užtikrina, kad kompetentingos institucijos veiksmingai vykdytų stebėseną ir imtųsi priemonių, būtinų užtikrinti, kad būtų laikomasi šios direktyvos, visų pirma 18 ir 20 straipsniuose nustatytų pareigų.

2. Kompetentingos institucijos, nagrinėdamos incidentus, dėl kurių pažeidžiamas asmens duomenų saugumas, glaudžiai bendradarbiauja su duomenų apsaugos institucijomis.

29 straipsnis

Esminių subjektų priežiūra ir vykdymo užtikrinimas

1. Valstybės narės užtikrina, kad priežiūros ar vykdymo užtikrinimo priemonės, taikomos svarbiausiems subjektams vykdant šioje direktyvoje nustatytas pareigas, būtų veiksmingos, proporcingos ir atgrasomosios, atsižvelgiant į kiekvieno atskiro atvejo aplinkybes.

2. Valstybės narės užtikrina, kad kompetentingos institucijos, vykdydamos savo priežiūros užduotis, susijusias su esminiais subjektais, turėtų įgaliojimus dėl tų subjektų:

   a) atlikti patikrinimus vietoje ir priežiūrą ne vietoje, įskaitant atsitiktinius patikrinimus;

   b) atlikti reguliarius auditus;

   c) atlikti tikslingus saugumo auditus, pagrįstus rizikos vertinimais arba prieinama informacija apie riziką;

   d) atlikti saugumo patikrinimus, pagrįstus objektyviais, nediskriminaciniais, sąžiningais ir skaidriais rizikos vertinimo kriterijais;

   e) prašyti pateikti informaciją, būtiną subjekto priimtoms kibernetinio saugumo priemonėms įvertinti, įskaitant dokumentais pagrįstą kibernetinio saugumo politiką, taip pat pareigos pranešti ENISA pagal 25 straipsnio 1 ir 2 dalis laikymąsi;

f) prašyti leisti susipažinti su duomenimis, dokumentais ar bet kokia 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.

3. Naudodamosi savo įgaliojimais pagal 2 dalies e–g punktus, kompetentingos institucijos nurodo prašymo tikslą ir prašomą informaciją.

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

(a) įspėti, kad subjektai nesilaiko šioje direktyvoje nustatytų pareigų;

(b) priimti privalomus nurodymus arba įsakymą, kuriuo reikalaujama, kad tie subjektai pašalintų nustatytus trūkumus arba šioje direktyvoje nustatytų pareigų pažeidimus;

(c) nurodyti tiems subjektams nutraukti veiksmus, kurie neatitinka šioje direktyvoje nustatytų pareigų, ir nebekartoti tokių veiksmų;

(d) nurodyti tiems subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų rizikos valdymo priemonės ir (arba) pareigos pranešti atitiktų 18 ir 20 straipsniuose nustatytas pareigas;

(e) nurodyti tiems subjektams informuoti fizinį (-ius) arba juridinį (-ius) asmenį (-is), kuriam (-iems) jie teikia paslaugas arba vykdo veiklą, kurioms gali pakenkti didelė kibernetinė grėsmė, apie visas galimas apsaugos ar taisomąsias priemones, kurių gali imtis tas (tie) fizinis (-iai) ar juridinis (-iai) asmuo (-enys), reaguodamas (-i) į tą grėsmę;

(f) nurodyti tiems subjektams per pagrįstą terminą įgyvendinti saugumo audito metu pateiktas rekomendacijas;

(g) paskirti stebėsenos pareigūną, kuriam per nustatytą laikotarpį pavestos aiškiai apibrėžtos užduotys, prižiūrėti, kaip laikomasi 18 ir 20 straipsniuose numatytų pareigų;

(h) nurodyti tiems subjektams konkrečiu būdu viešai paskelbti šioje direktyvoje nustatytų pareigų nevykdymo aspektus;

(i) padaryti viešą pareiškimą, kuriame nurodo už šioje direktyvoje nustatytos pareigos pažeidimą atsakingą (-us) juridinį (-ius) ir fizinį (-ius) asmenį (-is) ir to pažeidimo pobūdį;

(j) skirti arba prašyti, kad atitinkamos įstaigos ar teismai pagal nacionalinės teisės aktus skirtų administracinę baudą pagal 31 straipsnį, kartu su šios dalies a–i punktuose nurodytomis priemonėmis arba vietoj jų, atsižvelgiant į kiekvieno atskiro atvejo aplinkybes.

5. Jei pagal 4 dalies a–d ir f punktus patvirtinti vykdymo užtikrinimo veiksmai pasirodo neveiksmingi, valstybės narės užtikrina, kad kompetentingos institucijos turėtų įgaliojimus nustatyti terminą, iki kurio reikalaujama, kad esminis subjektas imtųsi būtinų veiksmų trūkumams pašalinti arba tų institucijų reikalavimams įvykdyti. Jei per nustatytą terminą nesiimama prašomų veiksmų, valstybės narės užtikrina, kad kompetentingos institucijos turėtų įgaliojimus:

(a) sustabdyti arba prašyti, kad sertifikavimo arba leidimus išduodanti įstaiga sustabdytų sertifikavimą arba įgaliojimą, susijusį su dalimi arba visomis esminės įstaigos teikiamomis paslaugomis ar veikla;

(b) nustatyti arba reikalauti, kad atitinkamos įstaigos ar teismai pagal nacionalinės teisės aktus nustatytų laikiną draudimą bet kuriam tame pagrindiniame subjekte vadovaujamas pareigas einančiam asmeniui arba teisiniam atstovui tame subjekte ir bet kuriam kitam fiziniam asmeniui, kuris laikomas atsakingu už pažeidimą, eiti vadovaujamas pareigas tame subjekte.

Šios sankcijos taikomos tik tol, kol subjektas imasi būtinų veiksmų trūkumams pašalinti arba kompetentingos institucijos, kuriai taikytos tokios sankcijos, reikalavimams įvykdyti.

6. Valstybės narės užtikrina, kad bet kuris fizinis asmuo, atsakingas už esminį subjektą arba veikiantis kaip jo atstovas, remdamasis jam suteiktais įgaliojimais, įgaliojimu priimti sprendimus jo vardu arba įgaliojimu vykdyti jo kontrolę, turėtų įgaliojimus užtikrinti, kad jis laikytųsi šioje direktyvoje nustatytų pareigų. Valstybės narės užtikrina, kad tie fiziniai asmenys galėtų būti traukiami atsakomybėn už jų pareigų užtikrinti šioje direktyvoje nustatytų pareigų vykdymą pažeidimą.

7. Imdamosi kokių nors vykdymo užtikrinimo veiksmų arba taikydamos sankcijas pagal 4 ir 5 dalis, kompetentingos institucijos gerbia teisę į gynybą ir atsižvelgia į kiekvieno atskiro atvejo aplinkybes ir tinkamai atsižvelgia bent į:

(a) pažeidimo sunkumą ir pažeistų nuostatų svarbą. Pažeidimai, kurie turėtų būti laikomi sunkiais: pakartotiniai pažeidimai, nepranešimas apie incidentus, turinčius didelį trikdantį poveikį, ir negebėjimas jų išspręsti, negebėjimas ištaisyti trūkumų pagal kompetentingų institucijų privalomus nurodymus, trukdymas vykdyti audito ar stebėsenos veiklą, kurią nurodė atlikti kompetentinga institucija po to, kai buvo nustatytas pažeidimas, neteisingos ar labai netikslios informacijos, susijusios su 18 ir 20 straipsniuose nustatytais rizikos valdymo reikalavimais arba pareigomis pranešti, pateikimas;

(b) pažeidimo trukmę, įskaitant pakartotinių pažeidimų elementą;

(c) faktiškai padarytą žalą ar patirtus nuostolius arba galimą žalą ar nuostolius, kurie galėjo būti patirti, jei juos galima nustatyti. Vertinant šį aspektą, be kita ko, atsižvelgiama į faktinius ar galimus finansinius ar ekonominius nuostolius, poveikį kitoms paslaugoms, paveiktų ar galimai paveiktų naudotojų skaičių;

(d) tai, ar pažeidimas padarytas tyčia, ar dėl aplaidumo;

(e) priemones, kurių subjektas ėmėsi siekdamas užkirsti kelią žalai ir (arba) nuostoliams arba juos sumažinti;

(f) patvirtintų elgesio kodeksų arba patvirtintų sertifikavimo mechanizmų laikymąsi;

(g) atsakingu (-ais) laikomo (-ų) fizinio (-ų) ar juridinio (-ų) asmens (-ų) bendradarbiavimo su kompetentingomis institucijomis lygį.

8. Kompetentingos institucijos išsamiai pagrindžia savo vykdymo užtikrinimo sprendimus. Prieš priimdamos tokius sprendimus kompetentingos institucijos atitinkamiems subjektams praneša savo preliminarias išvadas ir suteikia tiems subjektams pagrįstą laikotarpį pastaboms pateikti.

9. Valstybės narės užtikrina, kad jų kompetentingos institucijos informuotų atitinkamas konkrečios valstybės narės kompetentingas institucijas, paskirtas pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva], kai jos naudojasi savo priežiūros ir vykdymo užtikrinimo įgaliojimais, kuriais siekiama užtikrinti, kad esminis subjektas, kuris pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva] laikomas ypatingos svarbos subjektu arba lygiaverčiu ypatingos svarbos subjektui, laikytųsi šioje direktyvoje nustatytų pareigų. Kompetentingų institucijų prašymu pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva] kompetentingos institucijos gali naudotis savo priežiūros ir vykdymo užtikrinimo įgaliojimais esminio subjekto, kuris, kaip nustatyta, yra ypatingos svarbos arba lygiavertis, atžvilgiu.

30 straipsnis

Svarbių subjektų priežiūra ir jų pareigų vykdymo užtikrinimas

1. Gavusios įrodymus ar nuorodas, kad svarbus subjektas nesilaiko šioje direktyvoje, visų pirma 18 ir 20 straipsniuose, nustatytų pareigų, valstybės narės užtikrina, kad kompetentingos institucijos prireikus imtųsi veiksmų taikydamos *ex post* priežiūros priemones.

2. Valstybės narės užtikrina, kad kompetentingos institucijos, vykdydamos savo priežiūros užduotis, susijusias su svarbiais subjektais, turėtų įgaliojimus dėl tų subjektų:

   (a) atlikti patikrinimus vietoje ir vykdyti *ex post* priežiūrą ne vietoje;

   (b) atlikti tikslingus saugumo auditus, pagrįstus rizikos vertinimais arba prieinama informacija apie riziką;

   (c) atlikti saugumo patikrinimus, pagrįstus objektyviais, sąžiningais ir skaidriais rizikos vertinimo kriterijais;

   (d) prašyti pateikti bet kokią informaciją, būtiną subjekto kibernetinio saugumo priemonėms *ex post* įvertinti, įskaitant dokumentais pagrįstą kibernetinio saugumo politiką, taip pat įvertinti pareigos pranešti ENISA pagal 25 straipsnio 1 ir 2 dalis laikymąsi;

   (e) prašyti leisti susipažinti su duomenimis, dokumentais ir (arba) bet kokia informacija, reikalinga priežiūros užduotims atlikti.

3. Naudodamosi savo įgaliojimais pagal 2 dalies d arba e punktus, 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 įgaliojimus:

   (a) įspėti, kad subjektai nesilaiko šioje direktyvoje nustatytų pareigų;

   (b) priimti privalomus nurodymus arba įsakymą, kuriuo reikalaujama, kad tie subjektai pašalintų nustatytus trūkumus arba šioje direktyvoje nustatytų pareigų pažeidimą;

   (c) nurodyti tiems subjektams nutraukti veiksmus, kurie neatitinka šioje direktyvoje nustatytų pareigų, ir nebekartoti tokių veiksmų;

(d) nurodyti tiems subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų rizikos valdymo priemonės arba pareigos pranešti atitiktų 18 ir 20 straipsniuose nustatytas pareigas;

(e) nurodyti tiems subjektams informuoti fizinį (-ius) arba juridinį (-ius) asmenį (-is), kuriam (-iems) jie teikia paslaugas arba vykdo veiklą, kurioms gali pakenkti didelė kibernetinė grėsmė, apie visas galimas apsaugos ar taisomąsias priemones, kurių gali imtis tas (tie) fizinis (-iai) ar juridinis (-iai) asmuo (-enys), reaguodamas (-i) į tą grėsmę;

(f) nurodyti tiems subjektams per pagrįstą terminą įgyvendinti saugumo audito metu pateiktas rekomendacijas;

(g) nurodyti tiems subjektams konkrečiu būdu viešai paskelbti šioje direktyvoje nustatytų pareigų nevykdymo aspektus;

(h) padaryti viešą pareiškimą, kuriame nurodo už šioje direktyvoje nustatytos pareigos pažeidimą atsakingą (-us) juridinį (-ius) ir fizinį (-ius) asmenį (-is) ir to pažeidimo pobūdį;

(i) skirti arba prašyti, kad atitinkamos įstaigos ar teismai pagal nacionalinės teisės aktus skirtų administracinę baudą pagal 31 straipsnį, kartu su šios dalies a–i punktuose nurodytomis priemonėmis arba vietoj jų, atsižvelgiant į kiekvieno atskiro atvejo aplinkybes.

5. 29 straipsnio 6–8 dalys taip pat taikomos šiame straipsnyje numatytoms priežiūros ir vykdymo užtikrinimo priemonėms, skirtoms II priede išvardytiems svarbiems subjektams.

31 straipsnis

Bendrosios administracinių baudų skyrimo esminiams ir svarbiems subjektams sąlygos

1. Valstybės narės užtikrina, kad už šioje direktyvoje nustatytų pareigų pažeidimus esminiams ir svarbiems subjektams skiriamos administracinės baudos pagal šį straipsnį kiekvienu atskiru atveju būtų veiksmingos, proporcingos ir atgrasomosios.

2. Administracinės baudos, atsižvelgiant į kiekvieno atskiro atvejo aplinkybes, skiriamos kartu su 29 straipsnio 4 dalies a–i punktuose, 29 straipsnio 5 dalyje ir 30 straipsnio 4 dalies a–h punktuose nurodytomis priemonėmis arba vietoj jų.

3. Sprendžiant, ar skirti administracinę baudą, ir kiekvienu atskiru atveju priimant sprendimą dėl jos dydžio, deramai atsižvelgiama bent į 29 straipsnio 7 dalyje nurodytus aspektus.

4. Valstybės narės užtikrina, kad už 18 arba 20 straipsnyje nustatytų pareigų pažeidimus pagal šio straipsnio 2 ir 3 dalis būtų skiriamos administracinės baudos, kurios būtų ne mažesnės kaip 10 000 000 EUR arba ne didesnės kaip 2 proc. įmonės, kuriai tas esminis arba svarbus subjektas priklauso, bendros pasaulinės metinės apyvartos praėjusiais finansiniais metais, atsižvelgiant į tai, kuri suma yra didesnė.

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

6. Nedarant poveikio kompetentingų institucijų įgaliojimams pagal 29 ir 30 straipsnius, kiekviena valstybė narė gali nustatyti taisykles dėl to, ar ir kokiu mastu administracinės baudos gali būti skiriamos 4 straipsnio 23 dalyje nurodytiems viešojo administravimo subjektams, atsižvelgiant į šioje direktyvoje nustatytas pareigas.

32 straipsnis

Pažeidimai, susiję su asmens duomenų saugumo pažeidimu

1. Jeigu kompetentingos institucijos turi žinių, kad dėl esminio arba svarbaus subjekto padaryto 18 ir 20 straipsniuose nustatytų pareigų pažeidimo pažeistas asmens duomenų saugumas, kaip apibrėžta Reglamento (ES) 2016/679 4 straipsnio 12 dalyje, apie kurį pranešama pagal to reglamento 33 straipsnį, jos per pagrįstą laikotarpį informuoja priežiūros institucijas, kompetentingas pagal to reglamento 55 ir 56 straipsnius.

2. Jeigu priežiūros institucijos, kompetentingos pagal Reglamento (ES) 2016/679 55 ir 56 straipsnius, nusprendžia naudotis savo įgaliojimais pagal to reglamento 58 straipsnio i punktą ir skirti administracinę baudą, kompetentingos institucijos administracinės baudos už tą patį pažeidimą pagal šios direktyvos 31 straipsnį neskiria. Tačiau kompetentingos institucijos gali taikyti šios direktyvos 29 straipsnio 4 dalies a–i punktuose, 29 straipsnio 5 dalyje ir 30 straipsnio 4 dalies a–h punktuose numatytus vykdymo užtikrinimo veiksmus arba naudotis sankcijų taikymo įgaliojimais.

3. Jeigu priežiūros institucija, kompetentinga pagal Reglamentą (ES) 2016/679, yra įsteigta kitoje valstybėje narėje nei kompetentinga institucija, kompetentinga institucija gali informuoti toje pačioje valstybėje narėje įsteigtą priežiūros instituciją.

33 straipsnis

Sankcijos

1. 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 atgrasomosios.

2. Valstybės narės ne vėliau kaip per [dvejus] metus nuo šios direktyvos įsigaliojimo praneša Komisijai apie tas taisykles ir priemones ir nepagrįstai nedelsdamos informuoja ją apie visus vėlesnius joms įtakos turinčius pakeitimus.

34 straipsnis

Savitarpio pagalba

1. Kai esminis arba svarbus subjektas teikia paslaugas daugiau nei vienoje valstybėje narėje arba turi pagrindinę buveinę ar atstovą valstybėje narėje, tačiau jo tinklų ir informacinės sistemos yra vienoje ar keliose kitose valstybėse narėse, pagrindinės

buveinės ar kitos įstaigos arba atstovo valstybės narės kompetentinga institucija ir tų kitų valstybių narių kompetentingos institucijos prireikus bendradarbiauja ir padeda viena kitai. Tas bendradarbiavimas apima bent tai, kad:

(a) valstybės narės kompetentingos institucijos, taikančios priežiūros arba vykdymo užtikrinimo priemones, per bendrąjį informacinį centrą informuoja kitų atitinkamų valstybių narių kompetentingas institucijas ir su jomis konsultuojasi dėl priežiūros ir vykdymo užtikrinimo priemonių, kurių imtasi, ir tolesnių veiksmų pagal 29 ir 30 straipsnius;

(b) kompetentinga institucija gali prašyti kitos kompetentingos institucijos imtis 29 ir 30 straipsniuose nurodytų priežiūros arba vykdymo užtikrinimo priemonių;

(c) kompetentinga institucija, gavusi kitos kompetentingos institucijos pagrįstą prašymą, teikia kitai kompetentingai institucijai pagalbą, kad 29 ir 30 straipsniuose nurodyti priežiūros ar vykdymo užtikrinimo veiksmai galėtų būti įgyvendinami veiksmingai, efektyviai ir nuosekliai. Tokia 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 apsikeitus informacija su kitomis atitinkamomis institucijomis, ENISA ir Komisija nustatoma, kad institucija nėra kompetentinga suteikti prašomą pagalbą arba kad prašoma pagalba nėra proporcinga kompetentingos institucijos pagal 29 arba 30 straipsnį vykdomoms priežiūros užduotims.

2. Kai tinkama ir bendru sutarimu, skirtingų valstybių narių kompetentingos institucijos gali vykdyti 29 ir 30 straipsniuose nurodytus bendrus priežiūros veiksmus.

VII SKYRIUS

Pereinamojo laikotarpio ir baigiamosios nuostatos

35 straipsnis

Peržiūra

Komisija periodiškai peržiūri šios direktyvos taikymą ir teikia ataskaitą Europos Parlamentui ir Tarybai. Ataskaitoje visų pirma įvertinama I ir II prieduose nurodytų sektorių, pasektorių, subjektų dydžio ir rūšių svarba ekonomikos ir visuomenės veikimui kibernetinio saugumo atžvilgiu. Šiuo tikslu ir siekiant tolesnės pažangos vykdant strateginį ir operatyvinį bendradarbiavimą, Komisija atsižvelgia į Bendradarbiavimo grupės ir CSIRT tinklo ataskaitas apie patirtį, įgytą strateginiu ir operatyviniu lygmeniu. Pirmoji ataskaita pateikiama ne vėliau kaip... [54 mėnesiai po šios direktyvos įsigaliojimo dienos].

36 straipsnis

Įgaliojimų delegavimas

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

2. 18 straipsnio 6 dalyje ir 21 straipsnio 2 dalyje nurodyti įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami penkerių metų laikotarpiui nuo […]

3. Europos Parlamentas arba Taryba gali bet kada atšaukti 18 straipsnio 6 dalyje ir 21 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 18 straipsnio 6 dalį ir 21 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.

37 straipsnis

Komiteto procedūra

1. Komisijai padeda komitetas. Tas komitetas – komitetas, kaip apibrėžta 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.

38 straipsnis

Perkėlimas į nacionalinės teisės aktus

1. Valstybės narės ne vėliau kaip … [18 mėnesių nuo šios direktyvos įsigaliojimo dienos] priima ir paskelbia įstatymus ir kitus teisės aktus, būtinus, kad būtų laikomasi šios direktyvos. Apie tai jos nedelsdamos praneša Komisijai. Tas priemones jos taiko nuo ... [viena diena po pirmoje pastraipoje nurodytos datos].

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

39 straipsnis

Reglamento (ES) Nr. 910/2014 pakeitimas

Reglamento (ES) Nr. 910/2014 19 straipsnis išbraukiamas.

40 straipsnis

Direktyvos (ES) 2018/1972 pakeitimas

Direktyvos (ES) 2018/1972 40 ir 41 straipsniai išbraukiami.

41 straipsnis

Panaikinimas

Direktyva (ES) 2016/1148 panaikinama nuo ... [direktyvos perkėlimo į nacionalinę teisę galutinis terminas].

Nuorodos į Direktyvą (ES) 2016/1148 aiškinamos kaip nuorodos į šią direktyvą ir skaitomos pagal III priede pateiktą koreliacijos lentelę.

42 straipsnis

Įsigaliojimas

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

43 straipsnis

Adresatai

Ši direktyva skirta valstybėms narėms.

Priimta Briuselyje

Europos Parlamento vardu
Pirmininkas

Tarybos vardu
Pirmininkas

FINANSINĖ TEISĖS AKTO PASIŪLYMO PAŽYMA

Turinys

1. PASIŪLYMO (INICIATYVOS) STRUKTŪRA

1.1. Pasiūlymo (iniciatyvos) pavadinimas

Pasiūlymas dėl direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148

1.2. Atitinkama (-os) politikos sritis (-ys) *(programų grupė)*

Ryšių tinklai, turinys ir technologijos

1.3. Pasiūlymas (iniciatyva) susijęs (-usi) su:

☐ **nauju veiksmu**

☐ **nauju veiksmu, kai bus įgyvendintas bandomasis projektas ir (arba) atlikti parengiamieji veiksmai**[40]

☒ **esamo veiksmo galiojimo pratęsimu**

☐ **vieno ar daugiau veiksmų sujungimu arba nukreipimu į kitą / naują veiksmą**

1.4. Pasiūlymo (iniciatyvos) pagrindas

1.4.1. Trumpalaikiai arba ilgalaikiai poreikiai, įskaitant išsamų iniciatyvos įgyvendinimo pradinio etapo tvarkaraštį

Peržiūros tikslas – padidinti visapusiško Europos Sąjungoje veikiančių įmonių visuose atitinkamuose sektoriuose kibernetinio atsparumo lygį, sumažinti atsparumo neatitikimus visoje vidaus rinkoje sektoriuose, kuriems jau taikoma direktyva, ir pagerinti bendro informuotumo apie padėtį lygį bei kolektyvinius pasirengimo ir reagavimo pajėgumus.

1.4.2. Sąjungos dalyvavimo pridėtinė vertė (gali būti susijusi su įvairiais veiksniais, pvz., koordinavimo nauda, teisiniu tikrumu, didesniu veiksmingumu ar papildomumu). Šiame punkte „Sąjungos dalyvavimo pridėtinė vertė“ – dalyvaujant Sąjungai užtikrinama vertė, papildanti vertę, kuri būtų užtikrinta vien valstybių narių veiksmais.

Kibernetinis atsparumas Sąjungoje negali būti veiksmingas, jeigu bus laikomasi nevienodo nacionaliniu ar regioniniu lygmeniu izoliuoto požiūrio. TIS direktyva šis trūkumas buvo iš dalies išspręstas nacionaliniu ir Sąjungos lygmenimis nustatant tinklų ir informacinių sistemų saugumo sistemą. Tačiau atliekant pirmą periodinę TIS direktyvos peržiūrą atkreiptas dėmesys į įvairius būdingus trūkumus, dėl kurių galiausiai valstybėse narėse atsirado didelių skirtumų, susijusių su pajėgumais, planavimu ir apsaugos lygiu, kurie tuo pat metu daro poveikį panašių įmonių galimybėms vidaus rinkoje veikti vienodomis sąlygomis.

ES intervencija, apimanti daugiau nei dabartines TIS direktyvos priemones, iš esmės yra pateisinama dėl: i) tarpvalstybinio problemos pobūdžio; ii) ES veiksmų siekiant pagerinti ir palengvinti veiksmingą nacionalinę politiką potencialo; iii) suderintų ir bendradarbiavimu grindžiamų TIS politikos priemonių indėlio veiksmingai užtikrinant duomenų apsaugą ir privatumą.

[40] Kaip nurodyta Finansinio reglamento 58 straipsnio 2 dalies a arba b punkte.

Tad nustatyti tikslai gali būti geriau pasiekti imantis ES lygmens, o ne valstybių narių lygmens veiksmų.

1.4.3. Panašios patirties praeityje pamokos

TIS direktyva yra pirmoji horizontalioji vidaus rinkos priemonė, kuria siekiama didinti Sąjungos tinklų ir sistemų atsparumą kibernetinio saugumo rizikai. Ji jau labai prisidėjo prie bendro valstybių narių kibernetinio saugumo lygio didinimo. Tačiau direktyvos taikymo ir įgyvendinimo peržiūra atskleidė keletą trūkumų, kuriuos, be didėjančio skaitmeninimo ir poreikio imtis naujesnių atsakomųjų veiksmų, reikia spręsti persvarstytame teisės akte.

1.4.4. Suderinamumas ir galima sąveika su kitomis atitinkamomis priemonėmis

Naujasis pasiūlymas visiškai dera su kitomis susijusiomis iniciatyvomis, pavyzdžiui, pasiūlymu dėl reglamento dėl skaitmeninės veiklos atsparumo finansų sektoriuje (DORA) ir Esminių paslaugų operatorių atsparumo direktyvos pasiūlymu. Jis taip pat atitinka Europos elektroninių ryšių kodeksą, Bendrąjį duomenų apsaugos reglamentą ir eIDAS reglamentą.

Pasiūlymas yra esminė ES saugumo sąjungos strategijos sudedamoji dalis.

1.5. Trukmė ir finansinis poveikis

☐ **trukmė ribota**

– ☐ galioja nuo MMMM [MM DD] iki MMMM [MM DD],

– ☐ įsipareigojimų asignavimų finansinis poveikis nuo MMMM iki MMMM, o mokėjimų asignavimų – nuo MMMM iki MMMM.

☒ **trukmė neribota**

– Įgyvendinimo pradinis laikotarpis – nuo 2022 iki 2025 m.

– vėliau – visuotinis taikymas.

1.6. Numatytas (-i) valdymo būdas (-ai)[41]

Tiesioginis valdymas, vykdomas Komisijos:

– ☒ padalinių, įskaitant Sąjungos delegacijų darbuotojus;

– ☐ vykdomųjų įstaigų.

☐ **Pasidalijamasis valdymas** kartu su valstybėmis narėmis

☐ **Netiesioginis valdymas**, biudžeto vykdymo užduotis pavedant:

– ☐ trečiosioms valstybėms arba jų paskirtoms įstaigoms;

– ☐ tarptautinėms organizacijoms ir jų agentūroms (nurodyti);

– ☐ EIB ir Europos investicijų fondui;

– X☐ Finansinio reglamento 70 ir 71 straipsniuose nurodytiems organams;

– ☐ viešosios teisės subjektams;

– ☐ privatinės teisės reglamentuojamoms įstaigoms, kurioms pavesta teikti viešąsias paslaugas, jeigu jos pateikia pakankamas finansines garantijas;

– ☐ valstybės narės privatinės teisės reglamentuojamoms įstaigoms, kurioms pavesta įgyvendinti viešojo ir privačiojo sektorių partnerystę ir kurios pateikia pakankamas finansines garantijas;

– ☐ atitinkamame pagrindiniame akte nurodytiems asmenims, kuriems pavesta vykdyti konkrečius veiksmus BUSP srityje pagal ES sutarties V antraštinę dalį.

– *Jei nurodomas daugiau kaip vienas valdymo būdas, išsamią informaciją pateikti šio punkto pastabų skiltyje.*

Pastabos

Europos Sąjungos kibernetinio saugumo agentūra, ENISA, kuriai Kibernetinio saugumo aktu suteikti nauji nuolatiniai įgaliojimai, padėtų valstybėms narėms ir Komisijai įgyvendinti peržiūrėtą TIS direktyvą.

Dėl peržiūrėtos TIS direktyvos nuo 2022–2023 m. ENISA veiks papildomose veiklos srityse. Nors šios veiklos sritys būtų įtrauktos į ENISA bendrąsias užduotis pagal jos įgaliojimus, dėl jų agentūrai teks papildomas darbo krūvis. Konkrečiau, be dabartinių veiklos sričių, pagal Komisijos pasiūlymą dėl peržiūrėtos TIS direktyvos ENISA taip pat turės į savo darbo programą konkrečiai įtraukti šiuos veiksmus: i) sukurti ir tvarkyti Europos pažeidžiamumų registrą (pasiūlymo 6 straipsnio 2 dalis), ii) teikti sekretoriato paslaugas Europos ryšių

[41] Informacija apie valdymo būdus ir nuorodos į Finansinį reglamentą pateikiamos svetainėje „BudgWeb“ https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

palaikymo dėl kibernetinių krizių organizaciniam tinklui (CyCLONe) (pasiūlymo 14 straipsnis) ir parengti metinę ataskaitą dėl kibernetinio saugumo būklės ES (pasiūlymo 15 straipsnis), iii) remti valstybių narių tarpusavio vertinimų organizavimą (pasiūlymo 16 straipsnis), iv) rinkti apibendrintus duomenis apie incidentus iš valstybių narių ir teikti technines rekomendacijas (pasiūlymo 20 straipsnio 9 dalis), v) sukurti ir tvarkyti tarpvalstybines paslaugas teikiančių subjektų registrą (pasiūlymo 25 straipsnis).

Todėl nuo 2022 m. bus prašoma 5 papildomų etatų ekvivalentų su atitinkamu maždaug 0,61 mln. EUR biudžetu šioms naujoms pareigybėms padengti (žr. atskirą agentūrų finansinę pažymą).

2. VALDYMO PRIEMONĖS

2.1. Stebėsenos ir atskaitomybės taisyklės

Nurodyti dažnumą ir sąlygas.

Komisija periodiškai peržiūrės direktyvos taikymą ir teiks Europos Parlamentui ir Tarybai ataskaitas. Pirmoji ataskaita teikiama praėjus trejiems metams nuo direktyvos įsigaliojimo. Be to, Komisija įvertins, ar direktyva į nacionalinę teisę teisingai perkelta visose valstybėse narėse.

2.2. Valdymo ir kontrolės sistema (-os)

2.2.1. Valdymo būdo (-ų), finansavimo įgyvendinimo mechanizmo (-ai), mokėjimo tvarkos ir siūlomos kontrolės sistemos pagrindimas

Už politikos sritį atsakingas Ryšių tinklų, turinio ir technologijų GD skyrius valdys direktyvos įgyvendinimą.

2.2.2. Informacija apie nustatytą riziką ir jai sumažinti įdiegtą (-as) vidaus kontrolės sistemą (-as)

Labai maža rizika, nes TIS direktyvos ekosistema jau sukurta.

2.2.3. Kontrolės išlaidų efektyvumo apskaičiavimas ir pagrindimas (kontrolės sąnaudų ir susijusių valdomų lėšų vertės santykis) ir numatomo klaidų rizikos lygio vertinimas (atliekant mokėjimą ir užbaigiant programą)

Neaktualu. Naudojamas tik administracinis biudžetas („Bendrasis biudžetas“).

2.3. Sukčiavimo ir pažeidimų prevencijos priemonės

Nurodyti dabartines arba numatytas prevencijos ir apsaugos priemones, pvz., išdėstytas Kovos su sukčiavimu strategijoje.

Neaktualu. Naudojamas tik administracinis biudžetas („Bendrasis biudžetas“).

3. NUMATOMAS PASIŪLYMO (INICIATYVOS) FINANSINIS POVEIKIS

3.1. Atitinkama daugiametės finansinės programos išlaidų kategorija ir siūloma nauja biudžeto išlaidų eilutė (-ės)

Daugiametės finansinės programos išlaidų kategorija	Biudžeto eilutė	Išlaidų rūšis	Įnašas			
	Numeris [Išlaidų kategorija…7……...……]	DA / NDA[42]	ELPA šalių[43]	valstybių kandidačių[44]	trečiųjų valstybių	pagal Finansinio reglamento [21 straipsnio 2 dalies b punktą]
	20 02 06 valdymo išlaidos 20 02 06	NDA	NE	NE	NE	NE

[42] DA – diferencijuotieji asignavimai, NDA – nediferencijuotieji asignavimai.

[43] ELPA – Europos laisvosios prekybos asociacija.

[44] Valstybių kandidačių ir, kai taikoma, Vakarų Balkanų potencialių kandidačių.

3.2. Numatomas poveikis išlaidoms

3.2.1. Numatomo poveikio išlaidoms santrauka

mln. EUR (tūkstantųjų tikslumu)

Daugiametės finansinės programos išlaidų kategorija	<…>	[Išlaidų kategorija……...……]

			2021 m.	**2022 m.**	**2023 m.**	**2024 m.**	**2025 m.**	**2026 m.**	**2027 m.**	***Po 2027 m.***	**IŠ VISO**
Veiklos asignavimai (išskaidyti pagal 3.1 punkte išvardytas biudžeto eilutes)	Įsipareigojimai	(1)									
	Mokėjimai	(2)									
Administracinio pobūdžio asignavimai, finansuojami iš programos paketo lėšų[45]	Įsipareigojimai = Mokėjimai	(3)									
IŠ VISO asignavimų programos paketui	Įsipareigojimai	=1+3									
	Mokėjimai	=2+3									

Daugiametės finansinės programos išlaidų kategorija	7	„Administracinės išlaidos“ Posėdžiai: TIS Bendradarbiavimo grupės plenariniai posėdžiai paprastai vyksta 4 kartus per metus. Komisija sumoka 27 valstybių narių atstovų maitinimo ir kelionės išlaidas (po vieną atstovą iš kiekvienos valstybės narės). Vieno posėdžio išlaidos galėtų siekti iki 15 tūkst. EUR. Misijos: misijos yra susijusios su TIS direktyvos įgyvendinimo stebėsena. Pavyzdys: per vienus metus (2019 m. gegužės mėn. – 2020 m. liepos mėn.) turėjome surengti vadinamuosius TIS šalių vizitus ir apsilankyti visose 27 valstybėse narėse, kad

[45] Techninė ir (arba) administracinė parama bei išlaidos ES programų ir (arba) veiksmų įgyvendinimui remti (buvusios BA eilutės), netiesioginiai moksliniai tyrimai, tiesioginiai moksliniai tyrimai.

		aptartume TIS direktyvos įgyvendinimą visoje ES.

Šią dalį pildyti naudojant administracinio pobūdžio biudžeto duomenų lentelę, kuri pirmiausia bus pateikta finansinės teisės akto pasiūlymo pažymos priede ir įkelta į DECIDE tarnybų tarpusavio konsultacijoms.

mln. EUR (tūkstantųjų tikslumu)

		2021 m.	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	*Po 2027 m.*	IŠ VISO
Žmogiškieji ištekliai		1,14	1,14	1,14	1,14	1,14	1,14	**1,14**		**7,98**
Kitos administracinės išlaidos		**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**		**0,63**
IŠ VISO asignavimų pagal daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJĄ	(Iš viso įsipareigojimų = Iš viso mokėjimų)	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**		**8,61**

mln. EUR (tūkstantųjų tikslumu)

		2021 m.	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	*Po 2027 m.*	IŠ VISO
IŠ VISO asignavimų visose daugiametės finansinės programos **IŠLAIDŲ KATEGORIJOSE**	Įsipareigojimai									
	Mokėjimai									

3.2.2. Numatomo poveikio administracinio pobūdžio asignavimams santrauka

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimų nenaudojama

– ☐X Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimai naudojami taip:

mln. EUR (tūkstantųjų tikslumu)

Metai	**2021 m.**	**2022 m.**	**2023 m.**	**2024 m.**	**2025 m.**	**2026 m.**	**2027 m.**	**IŠ VISO**
Daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJA								
Žmogiškieji ištekliai	1,14	1,14	1,14	1,14	1,14	1,14	**1,14**	**7,98**
Kitos administracinės išlaidos	0,09	0,09	0,09	0,09	0,09	0,09	**0,09**	**0,63**
Daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJOS tarpinė suma	1,23	1,23	1,23	1,23	1,23	1,23	**1,23**	**8,61**
Neįtraukta į daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJĄ[46]								
Žmogiškieji ištekliai								
Kitos administracinio pobūdžio išlaidos								
Tarpinė suma, neįtraukta į daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJĄ								
IŠ VISO	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**8,61**

Žmogiškųjų išteklių ir kitų administracinio pobūdžio išlaidų asignavimų poreikiai bus tenkinami iš GD asignavimų, jau paskirtų priemonei valdyti ir (arba) perskirstytų generaliniame direktorate, ir prireikus finansuojami iš papildomų lėšų, kurios atsakingam GD gali būti skiriamos pagal metinę lėšų skyrimo procedūrą ir atsižvelgiant į biudžeto apribojimus.

46 Techninė ir (arba) administracinė parama bei išlaidos ES programų ir (arba) veiksmų įgyvendinimui remti (buvusios BA eilutės), netiesioginiai moksliniai tyrimai, tiesioginiai moksliniai tyrimai.

3.2.2.1. Numatomi žmogiškųjų išteklių poreikiai

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškųjų išteklių nenaudojama.

– X☐ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškieji ištekliai naudojami taip:

Sąmatą surašyti etatų vienetais

Metai		**2021 m.**	**2022 m.**	**2023 m.**	**2024 m.**	**2025 m.**	**2026 m.**	**2027 m.**
•Etatų plano pareigybės (pareigūnai ir laikinieji darbuotojai)								
Komisijos būstinė ir atstovybės		6	6	6	6	6	6	6
Delegacijos								
Moksliniai tyrimai								
• Išorės darbuotojai (etatų ekvivalentais: FTE) – CA, LA, SNE, INT ir JES [47] 7 išlaidų kategorija								
Finansuojama pagal daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJĄ	- būstinėje	3	3	3	3	3	3	3
	– delegacijose							
Finansuojama iš programos paketo lėšų [48]	- būstinėje							
	- delegacijose							
Moksliniai tyrimai								
Kita (nurodyti)								
IŠ VISO		**9**	**9**	**9**	**9**	**9**	**9**	**9**

Žmogiškųjų išteklių poreikiai bus tenkinami panaudojant GD darbuotojus, jau paskirtus veiksmui valdyti ir (arba) perskirstytus generaliniame direktorate, ir prireikus finansuojami iš papildomų lėšų, kurios atsakingam GD gali būti skiriamos pagal metinę lėšų skyrimo procedūrą ir atsižvelgiant į biudžeto apribojimus.

Vykdytinų užduočių aprašymas:

Pareigūnai ir laikinieji darbuotojai	• Deleguotųjų aktų rengimas pagal 18 straipsnio 6 dalį, 21 straipsnio 2 dalį, 36 straipsnį; • Įgyvendinimo aktų rengimas pagal 12 straipsnio 8 dalį, 18 straipsnio 5 dalį, 20 straipsnio 11 dalį; • TIS Bendradarbiavimo grupės sekretoriato paslaugų teikimas; • TIS Bendradarbiavimo grupės plenarinių posėdžių ir darbo grupės posėdžių organizavimas; • Valstybių narių darbo, susijusio su įvairiais dokumentais (gairėmis, priemonių rinkiniais ir pan.), koordinavimas; • Ryšių palaikymas su kitomis Komisijos tarnybomis, ENISA ir nacionalinėmis valdžios institucijomis siekiant įgyvendinti TIS direktyvą; • Nacionalinių metodų ir geriausios praktikos, atsižvelgiant į TIS direktyvos įgyvendinimą, analizė.
Išorės darbuotojai	Prireikus parama įgyvendinant visas pirmiau minėtas užduotis

[47] CA – sutartininkas („Contract Staff“), LA – vietinis darbuotojas („Local Staff“), SNE – deleguotasis nacionalinis ekspertas („Seconded National Expert“), INT – per agentūrą įdarbintas darbuotojas („agency staff“), JES – jaunesnysis delegacijos specialistas („Junior Professionals in Delegations“).

[48] Neviršijant viršutinės ribos, nustatytos išorės darbuotojams, finansuojamiems iš veiklos asignavimų (buvusių BA eilučių).

3.2.3. Trečiųjų šalių įnašai

Pasiūlyme (iniciatyvoje):

– X☐ nenumatyta bendro su trečiosiomis šalimis finansavimo

– ☐ numatytas trečiųjų šalių bendras finansavimas apskaičiuojamas taip:

Asignavimai mln. EUR (tūkstantųjų tikslumu)

Metai	**2021 m.**	**2022 m.**	**2023 m.**	**2024 m.**	**2025 m.**	**2026 m.**	**2027 m.**	**IŠ VISO**
Nurodyti bendrą finansavimą teikiančią įstaigą								
IŠ VISO bendrai finansuojamų asignavimų								

3.3. Numatomas poveikis pajamoms

– ☐X Pasiūlymas (iniciatyva) neturi finansinio poveikio pajamoms.

– ☐ Pasiūlymas (iniciatyva) turi finansinį poveikį:

☐ nuosaviems ištekliams

☐ kitoms pajamoms

nurodyti, jei pajamos priskirtos išlaidų eilutėms☐

mln. EUR (tūkstantųjų tikslumu)

Biudžeto pajamų eilutė:	Pasiūlymo (iniciatyvos) poveikis[49]						
	2021 m.	**2022 m.**	**2023 m.**	**2024 m.**	**2025 m.**	**2026 m.**	**2027 m.**
……. straipsnis							

Asignuotųjų pajamų atveju nurodyti biudžeto išlaidų eilutę (-es), kuriai (-oms) daromas poveikis.

Kitos pastabos (pvz., poveikio pajamoms apskaičiavimo metodas (formulė) arba kita informacija).

[49] Tradiciniai nuosavi ištekliai (muitai, cukraus mokesčiai) turi būti nurodomi grynosiomis sumomis, t. y. iš bendros sumos atskaičius 20 % surinkimo sąnaudų.

PRIEDAS
prie FINANSINĖS TEISĖS AKTO PASIŪLYMO PAŽYMOS

Pasiūlymo (iniciatyvos) pavadinimas

Pasiūlymas dėl direktyvos, kuria persvarstoma 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

……
……

1. REIKALINGŲ ŽMOGIŠKŲJŲ IŠTEKLIŲ SKAIČIUS IR SU JAIS SUSIJUSIOS SĄNAUDOS

2. KITŲ ADMINISTRACINIŲ IŠLAIDŲ SĄNAUDOS

3. APYTIKRIŲ IŠLAIDŲ APSKAIČIAVIMO METODAI

3.1 Žmogiškieji ištekliai

3.2 Kitos administracinės išlaidos

*Šis priedas, **kurį pildo visi su pasiūlymu (iniciatyva) susiję generaliniai direktoratai ir (arba) tarnybos**, turi būti pridedamas prie finansinės teisės akto pasiūlymo pažymos, kai pradedamos tarnybų tarpusavio konsultacijos.*

Duomenų lentelės naudojamos kaip finansinėje teisės akto pasiūlymo pažymoje pateiktų lentelių šaltinis. Jos skirtos tik naudoti Komisijoje.

1. Su reikalingais žmogiškaisiais ištekliais susijusios sąnaudos

☐ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškųjų išteklių nenaudojama.

X☐ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškieji ištekliai naudojami taip:

mln. EUR (tūkstantųjų tikslumu)

Daugiametės finansinės programos **7 IŠLAIDŲ KATEGORIJA**		**2021 m.**		**2022 m.**		**2023 m.**		**2024 m.**		**2025 m.**		**2026 m.**		**2027 m.**		**IŠ VISO**	
		Etatų vienetai	Asignavimai	Etatų vienetai	Asignavimai	Etatų vienetai	Asignavimai	Etatų vienetai	Asignavimai	Etatų vienetai	Asignavimai	Etatų vienetai	Asignavimai	Etatų vienetai	Asignavimai	Etatų vienetai	Asignavimai
• Etatų plano pareigybės (pareigūnai ir laikinieji darbuotojai)																	
Komisijos būstinė ir atstovybės	AD	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	42	6,3
	AST																
Sąjungos delegacijose	AD																
	AST																
• Išorės darbuotojai [50] 0,24																	
Bendrasis biudžetas	CA	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	21	1,68
	DNE																
	INT																
Sąjungos delegacijose	CA																
	LA																

[50] CA – sutartininkas („Contract Staff“), LA – vietinis darbuotojas („Local Staff“), SNE – deleguotasis nacionalinis ekspertas („Seconded National Expert“), INT – per agentūrą įdarbintas darbuotojas („Agency staff“); JES – jaunesnysis delegacijos specialistas („Junior Professionals in Delegations“).

	DNE																
	INT																
	JES																
Kitos biudžeto eilutės (*nurodyti*)																	
Daugiametės finansinės programos **7 IŠLAIDŲ KATEGORIJOS tarpinė suma**		9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	63	7,98

Žmogiškųjų išteklių poreikiai bus tenkinami panaudojant GD darbuotojus, jau paskirtus veiksmui valdyti ir (arba) perskirstytus generaliniame direktorate, ir prireikus finansuojami iš papildomų lėšų, kurios atsakingam GD gali būti skiriamos pagal metinę lėšų skyrimo procedūrą ir atsižvelgiant į biudžeto apribojimus.

Neįtraukta į daugiametės finansinė programos **7 IŠLAIDŲ KATEGORIJĄ**			**2021 m.**		**2022 m.**		**2023 m.**		**2024 m.**		**2025 m.**		**2025 m.**		**2025 m.**		**IŠ VISO**	
			Etatų vienetai	Asignavimai	Etatų vienetai	Asignavimai	Etatų vienetai	Asignavimai	Etatų vienetai	Asignavimai	Etatų vienetai	Asignavimai	Etatų vienetai	Asignavimai	Etatų vienetai	Asignavimai	Etatų vienetai	Asignavimai
• Etatų plano pareigybės (pareigūnai ir laikinieji darbuotojai)																		
Moksliniai tyrimai		AD																
		AST																
• Išorės darbuotojai[51]																		
Išorės personalas, finansuojamas iš veiklos asignavimų (buvusių BA eilučių).	- būstinėje	CA																
		DNE																
		INT																
	– Sąjungos delegacijose	CA																
		LA																
		DNE																
		INT																
		JES																
Moksliniai tyrimai)		CA																
		DNE																
		INT																

[51] CA – sutartininkas („Contract Staff“), LA – vietinis darbuotojas („Local Staff“), SNE – deleguotasis nacionalinis ekspertas („Seconded National Expert“), INT – per agentūrą įdarbintas darbuotojas („agency staff“), JPD – jaunesnysis delegacijos specialistas („Junior Professionals in Delegations“).

Kitos biudžeto eilutės (*nurodyti*)																	
Tarpinė suma, neįtraukta į daugiametės finansinės programos **7 IŠLAIDŲ KATEGORIJĄ**																	

Žmogiškųjų išteklių poreikiai bus tenkinami panaudojant GD darbuotojus, jau paskirtus veiksmui valdyti ir (arba) perskirstytus generaliniame direktorate, ir prireikus finansuojami iš papildomų lėšų, kurios atsakingam GD gali būti skiriamos pagal metinę lėšų skyrimo procedūrą ir atsižvelgiant į biudžeto apribojimus.

Numatomas poveikis ENISA žmogiškiesiems ištekliams

Europos Sąjungos kibernetinio saugumo agentūra, ENISA, kuriai Kibernetinio saugumo aktu suteikti nauji nuolatiniai įgaliojimai, padėtų valstybėms narėms ir Komisijai įgyvendinti peržiūrėtą TIS direktyvą.

Dėl peržiūrėtos TIS direktyvos nuo 2022–2023 m. ENISA veiks papildomose veiklos srityse. Nors šios veiklos sritys būtų įtrauktos į ENISA bendrąsias užduotis pagal jos įgaliojimus, dėl jų agentūrai teks papildomas darbo krūvis. Konkrečiau, be dabartinių veiklos sričių, pagal Komisijos pasiūlymą dėl peržiūrėtos TIS direktyvos ENISA taip pat turės į savo darbo programą konkrečiai įtraukti šiuos veiksmus: i) sukurti ir tvarkyti Europos pažeidžiamumų registrą (pasiūlymo 6 straipsnio 2 dalis), ii) teikti sekretoriato paslaugas Europos ryšių palaikymo dėl kibernetinių krizių organizaciniam tinklui (CyCLONe) (pasiūlymo 14 straipsnis) ir parengti metinę ataskaitą dėl kibernetinio saugumo būklės ES (pasiūlymo 15 straipsnis), iii) remti valstybių narių tarpusavio vertinimų organizavimą (pasiūlymo 16 straipsnis), iv) rinkti apibendrintus duomenis apie incidentus iš valstybių narių ir teikti technines rekomendacijas (pasiūlymo 20 straipsnio 9 dalis), v) sukurti ir tvarkyti tarpvalstybines paslaugas teikiančių subjektų registrą (pasiūlymo 25 straipsnis).

Todėl nuo 2022 m. bus prašoma 5 papildomų etatų ekvivalentų su atitinkamu maždaug 0,61 mln. EUR biudžetu šioms naujoms pareigybėms padengti (žr. atskirą agentūrų finansinę pažymą).

Todėl nuo 2022 m. bus prašoma 5 papildomų etatų ekvivalentų šioms naujoms pareigybėms padengti.

☐ Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimų nenaudojama

☐X Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimai naudojami taip:

mln. EUR (tūkstantųjų tikslumu)

	Metai **N**[52] **2022 m.**	Metai **N+1** **2023 m.**	Metai **N+2** **2024 m.**	Metai **N+3** **2025 m.**	Įterpti tiek metų, kiek reikia poveikio trukmei perteikti (žr. 1.6 punktą).			**IŠ VISO**
Laikinieji darbuotojai (AD lygio)	0,450	0,450	0,450	0,450	0,450	0,450		**2.7**

[52] N metai yra pasiūlymo (iniciatyvos) įgyvendinimo pradžios metai. Pakeiskite „N“ numatomais pirmaisiais įgyvendinimo metais (pavyzdžiui, 2021 m.). Atitinkamai pakeiskite vėlesnius metus.

Laikinieji darbuotojai (AST lygio)								
Sutartininkai	0,160	0,160	0,160	0,160	0,160	0,160		
Deleguotieji nacionaliniai ekspertai								**0,96**
IŠ VISO	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Personalo poreikiai (etato ekvivalentas):

	Metai **N**[53] **2022 m.**	Metai **N+1** **2023 m.**	Metai **N+2** **2024 m.**	Metai **N+3** **2025 m.**	Įterpti tiek metų, kiek reikia poveikio trukmei perteikti (žr. 1.6 punktą).	**IŠ VISO**
Laikinieji darbuotojai (AD lygio)	3	3	3	3	3	3		**18**
Laikinieji darbuotojai (AST lygio)								
Sutartininkai	2	2	2	2	2	2		**12**

[53] N metai yra pasiūlymo (iniciatyvos) įgyvendinimo pradžios metai. Pakeiskite „N“ numatomais pirmaisiais įgyvendinimo metais (pavyzdžiui, 2021 m.). Atitinkamai pakeiskite vėlesnius metus.

Deleguotieji nacionaliniai ekspertai								

IŠ VISO	**5**	**5**	**5**	**5**	**5**	**5**		**30**

2. Kitos administracinės išlaidos

☐ Pasiūlymui (iniciatyvai) įgyvendinti administraciniai asignavimai nenaudojami

X☐ Pasiūlymui (iniciatyvai) įgyvendinti administraciniai asignavimai naudojami taip:

mln. EUR (tūkstantųjų tikslumu)

Daugiametės finansinės programos **7 IŠLAIDŲ KATEGORIJA**	**2021**	**2022 m.**	**2023 m.**	**2024 m.**	**2025 m.**	**2026 m.**	**2027 m.**	**Iš viso**
Būstinėje:								
Misijų ir reprezentacinės išlaidos	0,03	0,03	0,03	0,03	0,03	0,03	0,03	**0,21**
Konferencijų ir posėdžių išlaidos	0,06	0,06	0,06	0,06	0,06	0,06	0,06	**0,42**
Komitetai[54]								
Tyrimai ir konsultacijos								
Informacija ir vadybos sistemos								

[54] Nurodyti komiteto rūšį ir kuriai grupei jis priklauso.

IRT įranga ir paslaugos[55]								
Kitos biudžeto eilutės (*prireikus nurodyti*)								
Sąjungos delegacijose								
Misijų, konferencijų ir reprezentacinės išlaidos								
Tęstinis darbuotojų mokymas								
Įsigijimas, nuoma ir susijusios išlaidos								
Įranga, baltai, biuro prekės ir paslaugos								
Daugiametės finansinės programos **7 IŠLAIDŲ KATEGORIJA**	0,09	0,09	0,09	0,09	0,09	0,09	0,09	**0,63**

[55] IRT – informacinės ir ryšių technologijos. Būtina konsultuotis su Informatikos GD.

mln. EUR (tūkstantųjų tikslumu)

Neįtraukta į daugiametės finansinė programos **7 IŠLAIDŲ KATEGORIJĄ**	**2021 m.**	**2022 m.**	**2023 m.**	**2024 m.**	**2025 m.**	**2026 m.**	**2027 m.**	**Iš viso**
Techninės ir administracinės pagalbos (nepasitelkiant išorės darbuotojų) išlaidos iš veiklai finansuoti skiriamų asignavimų (buvusios BA eilutės)								
- būstinėje								
– Sąjungos delegacijose								
Kitos valdymo išlaidos moksliniams tyrimams								
Kitos biudžeto eilutės (*prireikus nurodyti*)								
Tarpinė suma, neįtraukta į daugiametės finansinės programos **7 IŠLAIDŲ KATEGORIJĄ**								

IŠ VISO Daugiametės finansinės programos **7 IŠLAIDŲ KATEGORIJA ir neįtraukta į 7 IŠLAIDŲ KATEGORIJĄ**	1,23	1,23	1,23	1,23	1,23	1,23	1,23	**8,61**

Administracinių asignavimų poreikiai bus tenkinami panaudojant asignavimus, jau paskirtus priemonei valdyti ir (arba) perskirstytus, ir prireikus finansuojami iš papildomų lėšų, kurios atsakingam GD gali būti skiriamos pagal metinę asignavimų skyrimo procedūrą ir atsižvelgiant į esamus biudžeto apribojimus.

3. Apytikrių išlaidų apskaičiavimo metodai

3.1 Žmogiškieji ištekliai

Šioje dalyje nustatomas skaičiavimo metodas, taikomas siekiant įvertinti reikalingus žmogiškuosius išteklius (darbo krūvio prielaidos, įskaitant konkrečias darbo vietas (SYSPER 2 darbo vietų aprašas), darbuotojų kategorijos ir atitinkamos vidutinės sąnaudos)

Daugiametės finansinės programos **7 IŠLAIDŲ KATEGORIJA**
Pastaba. Kiekvienos būstinėje dirbančių darbuotojų kategorijos vidutinės sąnaudos nurodomos svetainėje „BudgWeb“: https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx.
• Pareigūnai ir laikinieji darbuotojai 6 pareigūnų etato ekvivalentai (vidutinės išlaidos 0,150) = 0,9 per metus - Deleguotųjų aktų rengimas pagal 18 straipsnio 6 dalį, 21 straipsnio 2 dalį, 36 straipsnį; - Įgyvendinimo aktų rengimas pagal 12 straipsnio 8 dalį, 18 straipsnio 5 dalį, 20 straipsnio 11 dalį; - TIS Bendradarbiavimo grupės sekretoriato paslaugų teikimas; - TIS Bendradarbiavimo grupės plenarinių posėdžių ir darbo grupės posėdžių organizavimas; - Valstybių narių darbo, susijusio su įvairiais dokumentais (gairėmis, priemonių rinkiniais ir pan.), koordinavimas; - Ryšių palaikymas su kitomis Komisijos tarnybomis, ENISA ir nacionalinėmis valdžios institucijomis siekiant įgyvendinti TIS direktyvą; - Nacionalinių metodų ir geriausios praktikos, atsižvelgiant į TIS direktyvos įgyvendinimą, analizė.
• Išorės darbuotojai 3 CA (vidutinės išlaidos 0,08) = 0,24 per metus - Prireikus parama įgyvendinant visas pirmiau minėtas užduotis

Neįtraukta į daugiametės finansinės programos **7 IŠLAIDŲ KATEGORIJĄ**
• Tik iš mokslinių tyrimų biudžeto finansuojamos pareigybės
• Išorės darbuotojai

3.2 Kitos administracinės išlaidos

Aprašykite kiekvienai biudžeto eilutei taikomą apskaičiavimo metodą,

visų pirma, svarbiausias prielaidas (pavyzdžiui, posėdžių skaičius per metus, vidutinės sąnaudos ir pan.)

Daugiametės finansinės programos **7 IŠLAIDŲ KATEGORIJA**
Posėdžiai: TIS Bendradarbiavimo grupės plenariniai posėdžiai paprastai vyksta 4 kartus per metus. Komisija sumoka 27 valstybių narių atstovų maitinimo ir kelionės išlaidas (po vieną atstovą iš kiekvienos valstybės narės). Vieno posėdžio išlaidos galėtų siekti iki 15 tūkst. EUR, o tai yra 60 tūkst. EUR per metus. Misijos: misijos yra susijusios su TIS direktyvos įgyvendinimo stebėsena. Pavyzdys: per vienus metus (2019 m. gegužės mėn. – 2020 m. liepos mėn.) turėjome surengti vadinamuosius TIS šalių vizitus ir apsilankyti visose 27 valstybėse narėse, kad aptartume TIS direktyvos įgyvendinimą visoje ES.

Neįtraukta į daugiametės finansinės programos **7 IŠLAIDŲ KATEGORIJĄ**

7 PRIEDAS

pridedamas prie
KOMISIJOS SPRENDIMO

dėl Komisijos tarnyboms skirtų Europos Sąjungos bendrojo biudžeto (Europos Komisijos skirsnio) vykdymo vidaus taisyklių

FINANSINĖ TEISĖS AKTO PASIŪLYMO PAŽYMA „AGENTŪROS“

Šis DJT apima prašymą nuo 2022 m. padidinti ENISA darbuotojų skaičių 5 etato ekvivalentais, kad būtų galima vykdyti papildomą veiklą, susijusią su TIS direktyvos įgyvendinimu. Ši veikla jau įtraukta į ENISA įgaliojimus.

Turinys

1. PASIŪLYMO (INICIATYVOS) STRUKTŪRA

1.1. Pasiūlymo (iniciatyvos) pavadinimas

Direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148, pasiūlymas

1.2. Atitinkama (-os) politikos sritis (-ys)

Ryšių tinklai, turinys ir technologijos

1.3. Pasiūlymas susijęs su:

☐ **nauju veiksmu**

☐ **nauju veiksmu, kai bus įgyvendintas bandomasis projektas ir (arba) atlikti parengiamieji veiksmai**[56]

☒ **esamos priemonės galiojimo pratęsimu**

☐ **vieno ar daugiau veiksmų sujungimu su kitu / nauju veiksmu**

1.4. Tikslas (-ai)

1.4.1. Bendras (-i) tikslas (-ai)

Peržiūros tikslas – padidinti visapusiško Europos Sąjungoje veikiančių įmonių visuose atitinkamuose sektoriuose kibernetinio atsparumo lygį, sumažinti atsparumo neatitikimus visoje vidaus rinkoje sektoriuose, kuriems jau taikoma direktyva, ir pagerinti bendro informuotumo apie padėtį lygį bei kolektyvinius pasirengimo ir reagavimo pajėgumus.

1.4.2. Konkretus (-ūs) tikslas (-ai)

Siekiant spręsti Europos Sąjungoje veikiančių įmonių mažo kibernetinio atsparumo problemą, konkretus tikslas yra užtikrinti, kad visų sektorių subjektai, kurie yra priklausomi nuo tinklų ir informacinių sistemų ir teikia pagrindines paslaugas ekonomikai ir visai visuomenei, turėtų imtis kibernetinio saugumo priemonių ir pranešti apie incidentus, kad būtų padidintas bendras kibernetinio atsparumo lygis visoje vidaus rinkoje.

Siekiant spręsti valstybių narių ir sektorių nevienodą atsparumo problemą, konkretus tikslas yra užtikrinti, kad visiems subjektams, veikiantiems sektoriuose, kuriems taikoma TIS teisinė sistema, kurių dydis panašus ir kurių vaidmuo panašus, būtų taikoma ta pati reguliavimo tvarka (tiek patenkantys į taikymo sritį, tiek už jos ribų), kad ir kokia jurisdikcija jiems priklausytų ES.

Siekiant užtikrinti, kad visi subjektai, veikiantys sektoriuose, kuriems taikoma TIS teisinė sistema, būtų įpareigoti laikytis tų pačių įsipareigojimų, grindžiamų rizikos valdymo koncepcija, kai kalbama apie saugumo priemones, ir turėtų pranešti apie visus incidentus pagal vienodus kriterijus, konkretūs tikslai yra užtikrinti, kad kompetentingos institucijos veiksmingiau užtikrintų teisės akte nustatytų taisyklių vykdymą, taikydamos suderintas priežiūros ir vykdymo užtikrinimo priemones, ir užtikrinti, kad visose valstybėse narėse

[56] Kaip nurodyta Finansinio reglamento 58 straipsnio 2 dalies a arba b punkte.

kompetentingoms institucijoms būtų skiriama panašaus lygio išteklių, kad jos galėtų vykdyti pagrindines TIS sistemos užduotis.

Siekiant spręsti bendro informuotumo apie padėtį ir bendro reagavimo į krizes trūkumo problemą, konkretus tikslas yra užtikrinti, kad valstybės narės keistųsi svarbiausia informacija, nustatant aiškias kompetentingų institucijų pareigas dalytis informacija ir bendradarbiauti kibernetinių grėsmių ir incidentų atvejais ir plėtojant bendrus Sąjungos operatyvinius reagavimo į krizes pajėgumus.

1.4.3. Numatomas (-i) rezultatas (-ai) ir poveikis

Nurodyti poveikį, kurį pasiūlymas (iniciatyva) turėtų padaryti tiksliniams gavėjams (tikslinėms grupėms).

Tikimasi, kad pasiūlymas duos didelės naudos: skaičiavimai rodo, kad dėl to kibernetinio saugumo incidentų sąnaudos gali sumažėti 11,3 mlrd. EUR. Taikymo sritis sektoriuose būtų gerokai išplėsta pagal TIS sistemą, tačiau, be pirmiau minėtų privalumų, našta, kuri gali atsirasti dėl TIS reikalavimų, visų pirma priežiūros požiūriu, taip pat būtų suderinta tiek naujų subjektų, kurie bus įtraukti, tiek kompetentingų institucijų atžvilgiu. Taip yra todėl, kad pagal naująją TIS sistemą būtų nustatytas dviejų lygmenų metodas, daugiausia dėmesio skiriant dideliems ir pagrindiniams subjektams ir diferencijuotai priežiūros tvarkai, kuri leistų vykdyti tik daugelio jų *ex post* priežiūrą, visų pirma tų, kurie laikomi „svarbiais“, tačiau nėra „esminiai“.

Apskritai pasiūlymas duotų abipusę naudą ir sinergiją, be to, tinkamiausia galimybė iš visų analizuotų politikos galimybių turi didžiausią potencialą užtikrinti didesnį ir nuoseklesnį pagrindinių subjektų visoje Sąjungoje kibernetinio atsparumo lygį, kuris galiausiai padėtų įmonėms ir visuomenei sutaupyti sąnaudų.

Be to, dėl pasiūlymo atitinkamos valstybių narių institucijos patirtų tam tikrų atitikties ir vykdymo užtikrinimo išlaidų (apskaičiuota, kad ištekliai iš viso padidės maždaug 20–30 proc.). Tačiau naujoji sistema taip pat būtų labai naudinga dėl geresnės pagrindinių įmonių apžvalgos ir sąveikos su jomis, tvirtesnio tarpvalstybinio operatyvinio bendradarbiavimo, taip pat savitarpio pagalbos ir tarpusavio vertinimo mechanizmų. Dėl to valstybėse narėse iš esmės padidėtų kibernetinio saugumo pajėgumai.

Apskaičiuota, kad įmonėms, kurios pateks į TIS sistemos taikymo sritį, pirmaisiais metais po naujos TIS sistemos įdiegimo joms reikėtų ne daugiau kaip 22 proc. padidinti dabartines IRT saugumo išlaidas (įmonių, kurioms jau taikoma dabartinė TIS direktyva, atveju tai būtų 12 proc.). Tačiau toks vidutinis IRT saugumo išlaidų padidėjimas suteiktų proporcingą naudą iš tokių investicijų, visų pirma dėl gerokai sumažėjusių kibernetinio saugumo incidentų išlaidų (numatoma, kad per dešimt metų ji sieks 118 mlrd. EUR).

Mažosios ir labai mažos įmonės nebūtų įtrauktos į TIS sistemos taikymo sritį. Galima tikėtis, kad vidutinės įmonės pirmaisiais metais nuo naujos tinklų ir informacijos saugumo sistemos įdiegimo padidins IRT saugumo išlaidas. Kartu padidinus saugumo reikalavimų šiems subjektams lygį taip pat būtų skatinami jų kibernetinio saugumo pajėgumai ir padedama gerinti IRT rizikos valdymą.

Poveikis būtų daromas nacionaliniams biudžetams ir administravimo subjektams: numatoma, kad trumpuoju ir vidutinės trukmės laikotarpiu ištekliai padidės maždaug 20–30 proc.

Jokio kito reikšmingo neigiamo poveikio nenumatoma. Tikimasi, kad pasiūlymu bus užtikrinti patikimesni kibernetinio saugumo pajėgumai, todėl jis turės didesnį švelnesnį poveikį incidentų, įskaitant duomenų saugumo pažeidimus, skaičiui ir sunkumui. Be to, tikėtina, kad tai turės teigiamą poveikį užtikrinant vienodas sąlygas visose valstybėse narėse visiems subjektams, patenkantiems į TIS taikymo sritį, ir sumažins kibernetinio saugumo informacijos asimetriją.

1.4.4. Veiklos rezultatų rodikliai

Nurodyti pažangos ir pasiekimų stebėsenos rodiklius.

Praėjus trejiems metams nuo naujojo TIS teisės akto įsigaliojimo, rodiklių vertinimą atliks Komisija, padedama ENISA ir Bendradarbiavimo grupės. Kai kurie stebėsenos rodikliai, kuriais remiantis būtų vertinama TIS peržiūros sėkmė, yra šie:

- Geresnis incidentų valdymas Imdamosi kibernetinio saugumo priemonių, įmonės gerina ne tik savo gebėjimą visiškai išvengti tam tikrų incidentų, bet ir reagavimo į incidentus pajėgumus. Todėl sėkmės rodikliai yra: i) trumpesnis vidutinis laikas, per kurį nustatomas incidentas, ii) laikas, per kurį organizacijos vidutiniškai atsigauna po incidento, ir iii) dėl incidento padarytos žalos vidutinės išlaidos.

- Didesnis aukščiausios įmonių vadovybės informuotumas apie kibernetinio saugumo riziką Nustačius reikalavimą, kad įmonės imtųsi priemonių, peržiūrėta TIS direktyva padėtų aukščiausiajai vadovybei geriau informuoti apie su kibernetiniu saugumu susijusią riziką. Tai galima įvertinti tiriant, kokiu mastu įmonės, patenkančios į TIS taikymo sritį, teikia pirmenybę kibernetiniam saugumui įmonės vidaus politikoje ir procesuose, kaip matyti iš vidaus dokumentų, atitinkamų mokymo programų ir darbuotojams skirtos informuotumo didinimo veiklos, ir teikia pirmenybę su saugumu susijusioms investicijoms į IRT. Visų svarbių ir svarbių subjektų vadovybė taip pat turėtų žinoti TIS direktyvoje nustatytas taisykles.

- Subalansuojant konkretiems sektoriams skirtas išlaidas IRT saugumo išlaidos įvairiuose ES sektoriuose labai skiriasi. Reikalaujant, kad daugiau sektorių įmonės imtųsi priemonių, nukrypimai nuo vidutinių konkrečiam sektoriui skirtų IRT saugumo išlaidų, kaip visų IRT išlaidų procentinė dalis, turėtų mažėti tarp sektorių ir tarp valstybių narių.

- Stipresnės kompetentingos institucijos ir glaudesnis bendradarbiavimas Persvarstyta TIS direktyva kompetentingoms institucijoms galėtų būti pavestos papildomos užduotys. Tai turėtų išmatuojamą poveikį kibernetinio saugumo agentūroms nacionaliniu lygmeniu skirtiems finansiniams ir žmogiškiesiems ištekliams, be to, tai turėtų turėti teigiamą poveikį kompetentingų institucijų gebėjimui aktyviai bendradarbiauti ir taip padidinti atvejų, kai kompetentingos institucijos bendradarbiauja tarpusavyje spręsdamos tarpvalstybinius incidentus arba vykdydamos bendrą priežiūros veiklą, skaičių.

- Dažnesnis keitimasis informacija Peržiūrėtas TIS taip pat pagerintų dalijimąsi informacija tarp įmonių ir su kompetentingomis institucijomis. Vienas iš peržiūros tikslų galėtų būti subjektų, dalyvaujančių įvairiose keitimosi informacija formose, skaičiaus didinimas.

1.5. Pasiūlymo (iniciatyvos) pagrindas

1.5.1. Trumpalaikiai arba ilgalaikiai poreikiai, įskaitant išsamų iniciatyvos įgyvendinimo pradinio etapo tvarkaraštį

Pasiūlymo tikslas – padidinti visapusiško Europos Sąjungoje veikiančių įmonių visuose atitinkamuose sektoriuose kibernetinio atsparumo lygį, sumažinti neatitikimus visoje vidaus rinkoje sektoriuose, kuriems jau taikoma direktyva, ir pagerinti bendro informuotumo apie padėtį lygį bei kolektyvinius pasirengimo ir reagavimo pajėgumus. Ji remsis per pastaruosius ketverius metus įgyvendinant Direktyvą (ES) 2016/1148 pasiektais rezultatais.

1.5.2. Sąjungos dalyvavimo pridėtinė vertė (gali būti susijusi su įvairiais veiksniais, pvz., koordinavimo nauda, teisiniu tikrumu, didesniu veiksmingumu ar papildomumu). Šiame punkte „Sąjungos dalyvavimo pridėtinė vertė“ – dalyvaujant Sąjungai užtikrinama vertė, papildanti vertę, kuri būtų užtikrinta vien valstybių narių veiksmais.

Kibernetinis atsparumas Sąjungoje negali būti veiksmingas, jeigu bus laikomasi nevienodo nacionaliniu ar regioniniu lygmeniu izoliuoto požiūrio. TIS direktyva šis trūkumas buvo iš dalies išspręstas nacionaliniu ir Sąjungos lygmenimis nustatant tinklų ir informacinių sistemų saugumo sistemą. Tačiau atliekant pirmą periodinę TIS direktyvos peržiūrą atkreiptas dėmesys į įvairius būdingus trūkumus, dėl kurių galiausiai valstybėse narėse atsirado didelių skirtumų, susijusių su pajėgumais, planavimu ir apsaugos lygiu, kurie tuo pat metu daro poveikį panašių įmonių galimybėms vidaus rinkoje veikti vienodomis sąlygomis.

ES intervencija, apimanti daugiau nei dabartines TIS direktyvos priemones, iš esmės yra pateisinama dėl: i) tarpvalstybinio problemos pobūdžio; ii) ES veiksmų siekiant pagerinti ir palengvinti veiksmingą nacionalinę politiką potencialo; iii) suderintų ir bendradarbiavimu grindžiamų TIS politikos priemonių indėlio veiksmingai užtikrinant duomenų apsaugą ir privatumą.

Tad nustatyti tikslai gali būti geriau pasiekti imantis ES lygmens, o ne valstybių narių lygmens veiksmų.

1.5.3. Panašios patirties praeityje pamokos

TIS direktyva yra pirmoji horizontalioji vidaus rinkos priemonė, kuria siekiama didinti Sąjungos tinklų ir sistemų atsparumą kibernetinio saugumo rizikai. Nuo TIS direktyvos įsigaliojimo 2016 m. ji jau labai prisidėjo prie bendro valstybių narių kibernetinio saugumo lygio didinimo. Tačiau direktyvos taikymo ir įgyvendinimo peržiūra atskleidė keletą trūkumų, kuriuos, be didėjančio skaitmeninimo ir poreikio imtis naujesnių atsakomųjų veiksmų, reikia šalinti persvarstytame teisės akte.

1.5.4. Suderinamumas su daugiamete finansine programa ir galima sinergija su kitomis atitinkamomis priemonėmis

Naujasis pasiūlymas visiškai dera su kitomis susijusiomis iniciatyvomis, pavyzdžiui, pasiūlymu dėl reglamento dėl skaitmeninės veiklos atsparumo finansų sektoriuje (DORA) ir Esminių paslaugų operatorių atsparumo direktyvos pasiūlymu. Jis taip pat atitinka Europos elektroninių ryšių kodeksą, Bendrąjį duomenų apsaugos reglamentą ir eIDAS reglamentą.

Pasiūlymas yra esminė ES saugumo sąjungos strategijos sudedamoji dalis.

1.5.5. Įvairių turimų finansavimo galimybių vertinimas, įskaitant perskirstymo mastą

Šioms ENISA užduotims vykdyti reikia specialių profilių ir papildomo darbo krūvio, kurių neįmanoma absorbuoti nepadidinus žmogiškųjų išteklių.

1.6. Pasiūlymo (iniciatyvos) trukmė ir finansinis poveikis

☐ **trukmė ribota**

– ☐ pasiūlymas (iniciatyva) galioja nuo MMMM [MM DD] iki MMMM [MM DD]

– ☐ finansinis poveikis nuo MMMM iki MMMM

☒ **trukmė neribota**

– Įgyvendinimo pradinis laikotarpis – nuo 2022 iki 2025 m.,

– vėliau – visuotinis taikymas.

1.7. Numatytas (-i) valdymo būdas (-ai)[57]

☒ **Tiesioginis valdymas**, vykdomas Komisijos:

– ☐ vykdomųjų įstaigų

☐ **Pasidalijamasis valdymas** kartu su valstybėmis narėmis

☐ X **Netiesioginis valdymas**, biudžeto vykdymo užduotis perduodant:

☐ tarptautinėms organizacijoms ir jų agentūroms (nurodyti);

☐ EIB ir Europos investicijų fondui;

☒ įstaigoms, nurodytoms 70 ir 71 straipsniuose;

☐ viešosios teisės subjektams;

☐ privatinės teisės reglamentuojamoms įstaigoms, kurioms pavesta teikti viešąsias paslaugas, jeigu jos pateikia pakankamas finansines garantijas;

☐ valstybės narės privatinės teisės reglamentuojamoms įstaigoms, kurioms pavesta įgyvendinti viešojo ir privačiojo sektorių partnerystę ir kurios pateikia pakankamas finansines garantijas;

☐ atitinkamame pagrindiniame akte nurodytiems asmenims, kuriems pavesta vykdyti konkrečius veiksmus BUSP srityje pagal ES sutarties V antraštinę dalį.

Pastabos

Europos Sąjungos kibernetinio saugumo agentūra, ENISA, kuriai Kibernetinio saugumo aktu suteikti nauji nuolatiniai įgaliojimai, padėtų valstybėms narėms ir Komisijai įgyvendinti peržiūrėtą TIS direktyvą.

Dėl peržiūrėtos TIS direktyvos nuo 2022–2023 m. ENISA veiks papildomose veiklos srityse. Nors šios veiklos sritys būtų įtrauktos į ENISA bendrąsias užduotis pagal jos įgaliojimus, dėl jų agentūrai teks papildomas darbo krūvis. Konkrečiau, be dabartinių veiksmų sričių, pagal Komisijos pasiūlymą dėl peržiūrėtos TIS direktyvos ENISA taip pat turės į savo darbo programą konkrečiai įtraukti šiuos veiksmus: i) sukurti ir tvarkyti Europos pažeidžiamumų registrą (pasiūlymo 6 straipsnio 2 dalis), ii) teikti sekretoriato paslaugas Europos ryšių palaikymo dėl kibernetinių krizių organizaciniam tinklui (CyCLONe) (pasiūlymo 14 straipsnis) ir parengti metinę ataskaitą dėl kibernetinio saugumo būklės ES

[57] Informacija apie valdymo būdus ir nuorodos į Finansinį reglamentą pateikiamos svetainėje „BudgWeb“ https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

(pasiūlymo 15 straipsnis), iii) remti valstybių narių tarpusavio vertinimų organizavimą (pasiūlymo 16 straipsnis), iv) rinkti apibendrintus duomenis apie incidentus iš valstybių narių ir teikti technines rekomendacijas (pasiūlymo 20 straipsnio 9 dalis), v) sukurti ir tvarkyti tarpvalstybines paslaugas teikiančių subjektų registrą (pasiūlymo 25 straipsnis).

Todėl nuo 2022 m. bus prašoma 5 papildomų etatų ekvivalentų su atitinkamu maždaug 0,61 mln. EUR biudžetu šioms naujoms pareigybėms padengti.

2. VALDYMO PRIEMONĖS

2.1. Stebėsenos ir atskaitomybės taisyklės

Nurodyti dažnumą ir sąlygas.

Komisija periodiškai peržiūrės direktyvos taikymą ir teiks Europos Parlamentui ir Tarybai ataskaitas. Pirmoji ataskaita teikiama praėjus trejiems metams nuo direktyvos įsigaliojimo.

Be to, Komisija įvertins, ar direktyva į nacionalinę teisę teisingai perkelta visose valstybėse narėse.

Vykdant pasiūlymo stebėseną ir teikiant ataskaitas bus laikomasi principų, nustatytų ENISA nuolatiniuose įgaliojimuose pagal Reglamentą (ES) 2019/881 (Kibernetinio saugumo aktas).

Planuojamai stebėsenai daugiausia naudojami ENISA, Bendradarbiavimo grupės, CSIRT tinklo ir valstybių narių valdžios institucijų duomenų šaltiniai. Be duomenų, kurie bus gaunami iš ENISA, Bendradarbiavimo grupės ir CSIRT tinklo ataskaitų (įskaitant metines veiklos ataskaitas), prireikus bus naudojamos specialios duomenų rinkimo priemonės (pavyzdžiui, nacionalinėms institucijoms skirti tyrimai, „Eurobarometro“ apklausa ir Kibernetinio mėnesio kampanijos bei visos Europos pratybų ataskaitos).

2.2. Valdymo ir kontrolės sistema (-os)

2.2.1. Valdymo būdo (-ų), finansavimo įgyvendinimo mechanizmo (-ai), mokėjimo tvarkos ir siūlomos kontrolės sistemos pagrindimas

Už politikos sritį atsakingas Ryšių tinklų, turinio ir technologijų GD skyrius valdys direktyvos įgyvendinimą.

Kalbant apie ENISA valdymą, Kibernetinio saugumo akto 15 straipsnyje pateiktas išsamus ENISA valdančiosios tarybos kontrolės funkcijų sąrašas.

Pagal Kibernetinio saugumo akto 31 straipsnį ENISA vykdomasis direktorius yra atsakingas už ENISA biudžeto vykdymą, o Komisijos vidaus auditorius ENISA atžvilgiu turi tuos pačius įgaliojimus kaip ir Komisijos padalinių atžvilgiu. ENISA valdančioji taryba pateikia nuomonę dėl ENISA finansinių ataskaitų.

2.2.2. Informacija apie nustatytą riziką ir jai sumažinti įdiegtą (-as) vidaus kontrolės sistemą (-as)

Labai maža rizika, nes TIS direktyvos ekosistema jau veikia ir jau apima ENISA, kuriai 2019 m. įsigaliojus Kibernetinio saugumo aktui suteikti nuolatiniai įgaliojimai.

2.2.3. Kontrolės išlaidų efektyvumo apskaičiavimas ir pagrindimas (kontrolės sąnaudų ir susijusių valdomų lėšų vertės santykis) ir numatomo klaidų rizikos lygio vertinimas (atliekant mokėjimą ir užbaigiant programą)

Prašomas biudžeto padidinimas taikomas 1 antraštinei daliai ir yra skirtas darbo užmokesčiui finansuoti. Tai reiškia, kad klaidų rizika mokėjimų lygmeniu yra labai maža.

2.3. Sukčiavimo ir pažeidimų prevencijos priemonės

Nurodyti dabartines arba numatytas prevencijos ir apsaugos priemones, pvz., išdėstytas Kovos su sukčiavimu strategijoje.

ENISA prevencijos ir apsaugos priemonės visų pirma būtų taikomos taip:

– Agentūros darbuotojai tikrina prašomus mokėjimus už bet kokią paslaugą arba tyrimus prieš atlikdami tuos mokėjimus, atsižvelgdami į visus sutartinius įsipareigojimus, ekonominius principus ir gerą finansinę arba valdymo praktiką. Nuostatos dėl kovos su sukčiavimu (priežiūra, atskaitomybės reikalavimai ir kt.) bus įtrauktos į visus Agentūros ir mokėjimų gavėjų sudarytus susitarimus ir sutartis.

– Siekiant kovoti su sukčiavimu, korupcija ir kita neteisėta veikla, be apribojimų taikomos 1999 m. gegužės 25 d. Europos Parlamento ir Tarybos reglamento (ES, Euratomas) Nr. 883/2013 dėl Europos kovos su sukčiavimu tarnybos (OLAF) atliekamų tyrimų nuostatos.

– Pagal SPS 33 straipsnį iki 2019 m. gruodžio 28 d. ENISA prisijungė prie 1999 m. gegužės 25 d. Europos Parlamento, Europos Sąjungos Tarybos ir Europos Bendrijų Komisijos tarpinstitucinio susitarimo dėl Europos kovos su sukčiavimu tarnybos (OLAF) atliekamų vidaus tyrimų. ENISA nedelsdama paskelbia atitinkamas visiems agentūros darbuotojams taikytinas nuostatas.

3. NUMATOMAS PASIŪLYMO (INICIATYVOS) FINANSINIS POVEIKIS

3.1. Atitinkama (-os) daugiametės finansinės programos išlaidų kategorija (-os) ir biudžeto išlaidų eilutė (-ės)

- Dabartinės biudžeto eilutės

Daugiametės finansinės programos išlaidų kategorijas ir biudžeto eilutes nurodyti eilės tvarka.

Daugiametės finansinės programos išlaidų kategorija	Biudžeto eilutė	Išlaidų rūšis	Įnašas			
	Numeris	DA / NDA[58]	ELPA šalių[59]	valstybių kandidačių[60]	trečiųjų valstybių	pagal Finansinio reglamento 21 straipsnio 2 dalies b punktą
2	02 10 04	/NDA	TAIP	NE	NE	/NE

- Prašomos sukurti naujos biudžeto eilutės

Daugiametės finansinės programos išlaidų kategorijas ir biudžeto eilutes nurodyti eilės tvarka.

Daugiametės finansinės programos	Biudžeto eilutė	Išlaidų rūšis	Įnašas			
	Numeris	DA / NDA	ELPA	valstybių	trečiųjų	pagal Finansinio reglamento 21

[58] DA – diferencijuotieji asignavimai, NDA – nediferencijuotieji asignavimai.

[59] ELPA – Europos laisvosios prekybos asociacija.

[60] Valstybių kandidačių ir, kai taikoma, Vakarų Balkanų potencialių kandidačių.

išlaidų kategorija			šalių	kandidačių	valstybių	straipsnio 2 dalies b punktą
	[XX.YY.YY.YY]		TAIP / NE	TAIP / NE	TAIP / NE	TAIP / NE

3.2. Numatomas poveikis išlaidoms

3.2.1. Numatomo poveikio išlaidoms santrauka

mln. EUR (tūkstantųjų tikslumu)

Daugiametės finansinės programos išlaidų kategorija	Numeris	[Išlaidų kategorija...2 Bendroji rinka, inovacijos ir skaitmeninė ekonomika.....]

[Įstaiga]: <…ENISA….>			Metai **N**[61] **2022 m.**	Metai **N+1** **2023 m.**	Metai **N+2** **2024 m.**	Metai **N+3** **2025 m.**	Įterpti tiek metų, kiek reikia poveikio trukmei perteikti (žr. 1.6 punktą). **2026 m.**	**2027 m.**		**IŠ VISO**
1 antraštinė dalis.	Įsipareigojimai	(1)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Mokėjimai	(2)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
2 antraštinė dalis.	Įsipareigojimai	(1a)								
	Mokėjimai	(2a)								
3 antraštinė dalis.	Įsipareigojimai	(3a)								
	Mokėjimai	(3b)								
IŠ VISO asignavimų skirta [įstaigai] <ENISA…….>	Įsipareigojimai	=1+1a +3a	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Mokėjimai	=2+2a +3b	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[61] N metai yra pasiūlymo (iniciatyvos) įgyvendinimo pradžios metai. Pakeiskite „N“ numatomais pirmaisiais įgyvendinimo metais (pavyzdžiui, 2021 m.). Atitinkamai pakeiskite vėlesnius metus.

Daugiametės finansinės programos išlaidų kategorija	**5**	„Administracinės išlaidos“

mln. EUR (tūkstantųjų tikslumu)

		Metai **N**	metai **N+1**	metai **N+2**	metai **N+3**	Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)			**IŠ VISO**
GD: <…….>									
• Žmogiškieji ištekliai									
• Kitos administracinės išlaidos									
IŠ VISO GD <…….>	Asignavimai								

IŠ VISO asignavimų pagal daugiametės finansinės programos **5 IŠLAIDŲ KATEGORIJĄ**	(Iš viso įsipareigojimų = Iš viso mokėjimų)								

mln. EUR (tūkstantųjų tikslumu)

		Metai **N**[62] **2022 m.**	Metai **N+1** **2023 m.**	Metai **N+2** **2024 m.**	Metai **N+3** **2025 m.**	Įterpti tiek metų, kiek reikia poveikio trukmei perteikti (žr. 1.6 punktą). **2026 m.**	**2027 m.**		**IŠ VISO**
IŠ VISO asignavimų pagal daugiametės finansinės programos **1–5 IŠLAIDŲ KATEGORIJAS**	Įsipareigojimai	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Mokėjimai	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[62] N metai yra pasiūlymo (iniciatyvos) įgyvendinimo pradžios metai. Pakeiskite „N“ numatomais pirmaisiais įgyvendinimo metais (pavyzdžiui, 2021 m.). Atitinkamai pakeiskite vėlesnius metus.

3.2.2. Numatomas poveikis [įstaigos] asignavimams

– ☐x Pasiūlymui (iniciatyvai) įgyvendinti veiklos asignavimai nenaudojami

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti veiklos asignavimai naudojami taip:

Įsipareigojimų asignavimas mln. EUR (tūkstantųjų tikslumu)

Nurodyti tikslus ir atliktus darbus ⇩			Metai **N**		metai **N+1**		metai **N+2**		metai **N+3**		Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)						**IŠ VISO**	
	ATLIKTI DARBAI																	
	Rūšis[63]	Vidutinės sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Bendras skaičius	Iš viso sąnaudų
1 KONKRETUS TIKSLAS[64]...																		
- Atlikti darbai																		
– Atliktas darbas																		
– Atliktas darbas																		
1 konkretaus tikslo tarpinė suma																		
2 KONKRETUS TIKSLAS...																		
- Atlikti darbai																		
2 konkretaus tikslo tarpinė suma																		
IŠ VISO SĄNAUDŲ																		

63 Atlikti darbai – tai būsimi produktai ir paslaugos (pvz., finansuota studentų mainų, nutiesta kelių kilometrų ir kt.).

64 Kaip apibūdinta 1.4.2 skirsnyje „Konkretus tikslas (-ai)…“.

3.2.3. Numatomas poveikis ENISA žmogiškiesiems ištekliams

3.2.3.1. Santrauka

Dėl peržiūrėtos TIS direktyvos nuo 2022–2023 m. ENISA vykdys papildomas užduotis. Nors šios užduotys būtų įtrauktos į ENISA įgaliojimus, dėl jų agentūrai teks papildomas darbo krūvis. Tiksliau tariant, be dabartinių užduočių, pagal Komisijos pasiūlymą dėl persvarstytos TIS direktyvos ENISA bus pavesta, be kita ko, i) sukurti ir tvarkyti Europos pažeidžiamumų registrą (6 straipsnio 2 dalis), ii) teikti sekretoriato paslaugas Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklui (CyCLONe), (14 straipsnis) ir parengti metinę ataskaitą dėl kibernetinio saugumo ES būklės (15 straipsnis), iii) remti valstybių narių tarpusavio vertinimų organizavimą (16 straipsnis), iv) rinkti apibendrintus duomenis apie incidentus iš valstybių narių ir teikti tarpvalstybines rekomendacijas (20 straipsnio 9 dalis), v) sukurti ir tvarkyti tarpvalstybines paslaugas teikiančių subjektų registrą (25 straipsnis).

Todėl nuo 2022 m. bus prašoma 5 papildomų etatų ekvivalentų šioms naujoms pareigybėms padengti.

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimų nenaudojama

– ☐X Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimai naudojami taip:

mln. EUR (tūkstantųjų tikslumu)

	Metai **N**[65] **2022 m.**	Metai **N+1** **2023 m.**	Metai **N+2** **2024 m.**	Metai **N+3** **2025 m.**	Įterpti tiek metų, kiek reikia poveikio trukmei perteikti (žr. 1.6 punktą). **2026 m.**	**2027 m.**		**IŠ VISO**
Laikinieji darbuotojai (AD lygio)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Laikinieji darbuotojai (AST lygio)								
Sutartininkai	0,160	0,160	0,160	0,160	0,160	0,160		**0,96**
Deleguotieji nacionaliniai ekspertai								
IŠ VISO	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

65 N metai yra pasiūlymo (iniciatyvos) įgyvendinimo pradžios metai. Pakeiskite „N“ numatomais pirmaisiais įgyvendinimo metais (pavyzdžiui, 2021 m.). Atitinkamai pakeiskite vėlesnius metus.

Personalo poreikiai (etato ekvivalentais):

	Metai **N**[66] **2022 m.**	Metai **N+1** **2023 m.**	Metai **N+2** **2024 m.**	Metai **N+3** **2025 m.**	Įterpti tiek metų, kiek reikia poveikio trukmei perteikti (žr. 1.6 punktą). **2026 m.**	**2027 m.**		**IŠ VISO**
Laikinieji darbuotojai (AD lygio)	3	3	3	3	3	3		**18**
Laikinieji darbuotojai (AST lygio)								
Sutartininkai	2	2	2	2	2	2		**12**
Deleguotieji nacionaliniai ekspertai								
IŠ VISO	**5**	**5**	**5**	**5**	**5**	**5**		**30**

3.2.3.2. Numatomi pagrindinio GD žmogiškųjų išteklių poreikiai

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškųjų išteklių nenaudojama.

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškieji ištekliai naudojami taip:

Sąmatą nurodyti sveikaisiais skaičiais (arba ne smulkiau nei dešimtųjų tikslumu)

	Metai **N**	metai **N+1**	Metai **N+2**	Metai **N+3**	Įterpti tiek metų, kiek reikia poveikio trukmei perteikti (žr. 1.6 punktą).		
• **Etatų plano pareigybės (pareigūnai ir laikinieji darbuotojai)**							
XX 01 01 01 (Komisijos būstinė ir atstovybės)							
XX 01 01 02 (Delegacijos)							
XX 01 05 01 (Netiesioginiai moksliniai tyrimai)							
10 01 05 01 (Tiesioginiai moksliniai tyrimai)							
• **Išorės darbuotojai (etatų vienetais)**[67]							

66 N metai yra pasiūlymo (iniciatyvos) įgyvendinimo pradžios metai. Pakeiskite „N“ numatomais pirmaisiais įgyvendinimo metais (pavyzdžiui, 2021 m.). Atitinkamai pakeiskite vėlesnius metus.

XX 01 02 01 (AC, END, INT finansuojami iš bendrojo biudžeto)								
XX 01 02 02 (CA, LA, SNE, INT ir JPD delegacijose)								
XX 01 04 ***mm***[68]	- būstinėje[69]							
	– delegacijose							
XX 01 05 02 (CA, SNE, INT – netiesioginiai moksliniai tyrimai)								
10 01 05 02 (CA, INT, SNE – tiesioginiai moksliniai tyrimai)								
Kitos biudžeto eilutės (nurodyti)								
IŠ VISO								

XX yra atitinkama politikos sritis arba biudžeto antraštinė dalis.

Žmogiškųjų išteklių poreikiai bus tenkinami panaudojant GD darbuotojus, jau paskirtus priemonei valdyti ir (arba) perskirstytus generaliniame direktorate, ir prireikus finansuojami iš papildomų lėšų, kurios atsakingam GD gali būti skiriamos pagal metinę lėšų skyrimo procedūrą ir atsižvelgiant į biudžeto apribojimus.

Vykdytinų užduočių aprašymas:

Pareigūnai ir laikinieji darbuotojai	
Išorės darbuotojai	

V priedo 3 skirsnyje turėtų būti pateiktas etato ekvivalentų išlaidų apskaičiavimo aprašymas.

67 CA – sutartininkas („Contract Staff“), LA – vietos darbuotojas („Local Staff“), SNE – deleguotasis nacionalinis ekspertas („Seconded National Expert“), INT – per agentūrą įdarbintas darbuotojas („agency staff“), JPD – jaunesnysis delegacijos specialistas („Junior Professionals in Delegations“).

68 Neviršijant viršutinės ribos, nustatytos išorės darbuotojams, finansuojamiems iš veiklos asignavimų (buvusių BA eilučių).

69 Paprastai struktūrinių fondų, Europos žemės ūkio fondo kaimo plėtrai (EŽŪFKP) ir Europos žuvininkystės fondo (EŽF) atveju.

3.2.4. Suderinamumas su dabartine daugiamete finansine programa

– ☐X Pasiūlymas (iniciatyva) atitinka dabartinę daugiametę finansinę programą.

– ☐ Atsižvelgiant į pasiūlymą (iniciatyvą), reikės pakeisti daugiametės finansinės programos atitinkamos išlaidų kategorijos programavimą.

Paaiškinti, kaip reikia pakeisti programavimą, ir nurodyti atitinkamas biudžeto eilutes bei sumas. Pasiūlymas dera su 2021–2027 m. DFP. Biudžetas, kurio prašoma ENISA žmogiškųjų išteklių didinimui padengti, bus kompensuotas ta pačia suma sumažinant Skaitmeninės Europos programos (SEP) toje pačioje išlaidų kategorijoje biudžetą.

– ☐ Įgyvendinant pasiūlymą (iniciatyvą) būtina taikyti lankstumo priemonę arba patikslinti daugiametę finansinę programą[70].

Paaiškinti, ką reikia atlikti, ir nurodyti atitinkamas išlaidų kategorijas, biudžeto eilutes ir sumas.

3.2.5. Trečiųjų šalių dalyvavimas finansavimo veikloje

– Pasiūlyme / iniciatyvoje nenumatyta bendro su trečiosiomis šalimis finansavimo.

– Pasiūlyme / iniciatyvoje numatytas toks bendras finansavimas:

mln. EUR (tūkstantųjų tikslumu)

	Metai **N**	metai **N+1**	metai **N+2**	metai **N+3**	Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)			Iš viso
Nurodyti bendrą finansavimą teikiančią įstaigą								
IŠ VISO bendrai finansuojamų asignavimų								

[70] Žr. Tarybos reglamento (ES, Euratomas) Nr. 1311/2013, kuriuo nustatoma 2014–2020 m. daugiametė finansinė programa, 11 ir 17 straipsnius.

3.3. Numatomas poveikis pajamoms

– ☐ Pasiūlymas (iniciatyva) neturi finansinio poveikio pajamoms.

– ☐ Pasiūlymas (iniciatyva) turi finansinį poveikį:

☐ nuosaviems ištekliams

☐ kitoms pajamoms

nurodyti, jei pajamos priskirtos išlaidų eilutėms

mln. EUR (tūkstantųjų tikslumu)

Biudžeto pajamų eilutė:	Einamųjų finansinių metų asignavimai	Pasiūlymo (iniciatyvos) poveikis[71]						
		metai **N**	metai **N+1**	metai **N+2**	metai **N+3**	Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)		
……. straipsnis								

Įvairių asignuotųjų pajamų atveju nurodyti biudžeto išlaidų eilutę (-es), kuriai (-ioms) daromas poveikis.

Nurodyti poveikio pajamoms apskaičiavimo metodą.

[71] Tradiciniai nuosavi ištekliai (muitai, cukraus mokesčiai) turi būti nurodomi grynosiomis sumomis, t. y. iš bendros sumos atskaičius 20 % surinkimo sąnaudų.