Europos Parlamentas
2019-2024

Plenarinio posėdžio dokumentas

A9-0313/2021

04.11.2021

***I
PRANEŠIMAS

dėl pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Pramonės, mokslinių tyrimų ir energetikos komitetas

Pranešėjas: Bart Groothuis

Nuomonės referentas (*):
Lukas Mandl, Piliečių laisvių, teisingumo ir vidaus reikalų komitetas

(*) Susijusių komitetų procedūra. Darbo tvarkos taisyklių 57 straipsnis

Procedūrų sutartiniai ženklai

*	Konsultavimosi procedūra
***	Pritarimo procedūra
***I	Įprasta teisėkūros procedūra (pirmasis svarstymas)
***II	Įprasta teisėkūros procedūra (antrasis svarstymas)
***III	Įprasta teisėkūros procedūra (trečiasis svarstymas)

(Procedūra pasirenkama atsižvelgiant į teisės akto projekte pasiūlytą teisinį pagrindą.)

Teisės akto projekto pakeitimai

Parlamento pakeitimai, išdėstomi dviejuose stulpeliuose

Išbrauktos teksto dalys žymimos ***pusjuodžiu kursyvu*** kairiajame stulpelyje. Pakeitimai žymimi ***pusjuodžiu kursyvu*** abiejuose stulpeliuose. Naujas tekstas žymimas ***pusjuodžiu kursyvu*** dešiniajame stulpelyje.

Kiekvieno pakeitimo antraštės pirmoje ir antroje eilutėse nurodoma atitinkama svarstomo teisės akto projekto dalis. Jei pakeitimas susijęs su esamu teisės aktu, kurį siekiama pakeisti teisės akto projektu, antraštėje pridedamos trečia ir ketvirta eilutės, kuriose atitinkamai nurodomas esamas teisės aktas ir keičiama šio teisės akto dalis.

Parlamento pakeitimai, pateikiami konsoliduoto teksto forma

Naujos teksto dalys žymimos ***pusjuodžiu kursyvu***. Išbrauktos teksto dalys nurodomos simboliu „▌“ arba perbraukiamos. Pakeistos teksto dalys nurodomos naują tekstą pažymint ***pusjuodžiu kursyvu***, o ankstesnį nereikalingą tekstą išbraukiant arba perbraukiant.
Nežymimi tik grynai techninio pobūdžio pakeitimai, kuriuos daro tarnybos, siekdamos parengti galutinį tekstą.

TURINYS

Psl.

EUROPOS PARLAMENTO TEISĖKŪROS REZOLIUCIJOS PROJEKTAS

dėl pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

(Įprasta teisėkūros procedūra: pirmasis svarstymas)

Europos Parlamentas,

– atsižvelgdamas į Komisijos pasiūlymą Europos Parlamentui ir Tarybai (COM(2020)0823),

– atsižvelgdamas į Sutarties dėl Europos Sąjungos veikimo 294 straipsnio 2 dalį ir 114 straipsnį, pagal kuriuos Komisija pateikė pasiūlymą Parlamentui (C9-0422/2020),

– atsižvelgdamas į Sutarties dėl Europos Sąjungos veikimo 294 straipsnio 3 dalį,

– atsižvelgdamas į 2021 m. balandžio 27 d. Europos ekonomikos ir socialinių reikalų komiteto nuomonę[1],

– pasikonsultavęs su Regionų komitetu,

– atsižvelgdamas į Darbo tvarkos taisyklių 59 straipsnį,

– atsižvelgdamas į Piliečių laisvių, teisingumo ir vidaus reikalų komiteto, Užsienio reikalų komiteto, Vidaus rinkos ir vartotojų apsaugos komiteto ir Transporto ir turizmo komiteto nuomones,

– atsižvelgdamas į Pramonės, mokslinių tyrimų ir energetikos komiteto pranešimą (A9-0313/2021),

1. priima per pirmąjį svarstymą toliau pateiktą poziciją;

2. ragina Komisiją dar kartą perduoti klausimą svarstyti Parlamentui, jei ji savo pasiūlymą pakeičia nauju tekstu, jį keičia iš esmės arba ketina jį keisti iš esmės;

3. paveda Pirmininkui perduoti Parlamento poziciją Tarybai, Komisijai ir nacionaliniams parlamentams.

[1] OL C 286, 2021 7 16, p. 170.

Pakeitimas 1

Pasiūlymas dėl direktyvos
Antraštinė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
Pasiūlymas	Pasiūlymas
EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA	EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA
dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148	dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti ***(TIS 2 direktyva)***, kuria panaikinama Direktyva (ES) 2016/1148

Pakeitimas 2

Pasiūlymas dėl direktyvos
1 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(1) Europos Parlamento ir Tarybos direktyva (ES) 2016/1148[11] ***(dažnai vadinama „TIS direktyva“)*** 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 Sąjungos ***saugumo ir veiksmingo jos*** ekonomikos ir visuomenės veikimo;
[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). 1).	[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). 1).

Pakeitimas 3

Pasiūlymas dėl direktyvos
3 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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. ***Be to, kibernetinis saugumas yra daugelio ypatingos svarbos sektorių bazinė didelio poveikio priemonė siekiant sėkmingai vykdyti skaitmeninę transformaciją ir visapusiškai pasinaudoti skaitmeninimo teikiama ekonomine, socialine ir tvarumo nauda;***

Pakeitimas 4

Pasiūlymas dėl direktyvos
3 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(3a) kilus didelio masto kibernetinio saugumo incidentams ir krizėms Sąjungos lygmeniu, dėl didelės sektorių ir šalių tarpusavio priklausomybės reikia imtis koordinuotų veiksmų, kad būtų užtikrintas greitas ir veiksmingas reagavimas Kadangi kibernetinės grėsmės gali kilti už Sąjungos ribų, siekiant užtikrinti Sąjungos saugumą viduje ir už jos ribų būtina turėti kibernetinėms

	grėsmėms atsparius tinklus ir informacines sistemas bei prieinamus, konfidencialius ir vientisus duomenis. Sąjungos siekis įgyti svarbesnį geopolitinį vaidmenį taip pat priklauso nuo patikimos kibernetinės gynybos ir atgrasymo, įskaitant gebėjimą laiku ir veiksmingai nustatyti kenkėjiškus veiksmus ir tinkamai į juos reaguoti;

Pakeitimas 5

Pasiūlymas dėl direktyvos
5 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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. ***Galiausiai dėl tų skirtumų kai kurios valstybės narės galėtų tapti labiau paveikios kibernetinio saugumo grėsmėms, įskaitant galimą šalutinį poveikį visoje Sąjungoje.*** 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 ***(TIS 2 direktyva)***;

Pakeitimas 6

Pasiūlymas dėl direktyvos
6 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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];	(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 ***užkirsti kelią nusikalstamoms veikoms, jas*** tirti bei išsiaiškinti 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];
[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).	[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).

Pakeitimas 7

Pasiūlymas dėl direktyvos
7 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(7) panaikinus Direktyvą (ES) 2016/1148, taikymo sritis sektoriams, atsižvelgiant į 4–6 konstatuojamosiose dalyse išvardytas aplinkybes, turėtų būti praplėsta, kad apimtų platesnį ekonomikos	(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;

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. ***Rizikos valdymo reikalavimai ir pareigos pranešti*** 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;

Pakeitimas 8

Pasiūlymas dėl direktyvos
8 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;***	(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.

[15] 2003 m. gegužės 6 d. Komisijos

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

Pakeitimas 9

Pasiūlymas dėl direktyvos
9 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;***	(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.

Pakeitimas 10

Pasiūlymas dėl direktyvos
9 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(9a) valstybės narės turėtų sudaryti visų esminių ir svarbių subjektų sąrašą. Į tą sąrašą turėtų būti įtraukti subjektai, atitinkantys bendrai taikomus su dydžiu susijusius kriterijus, taip pat mažosios ir labai mažos įmonės, kurios atitinka tam tikrus kriterijus, parodančius jų esminį vaidmenį valstybių narių ekonomikoje ar visuomenėje. Kad reagavimo į kompiuterių saugumo incidentus tarnybos (CSIRT) ir kompetentingos institucijos galėtų teikti pagalbą ir įspėti subjektus apie kibernetinius incidentus, kurie galėtų jiems daryti poveikį, svarbu, kad tos institucijos turėtų teisingus subjektų kontaktinius duomenis. Todėl esminiai ir svarbūs subjektai kompetentingoms institucijoms turėtų pateikti bent tokią informaciją: subjekto pavadinimą, adresą

	ir aktualius kontaktinius duomenis, įskaitant e. pašto adresus, IP adresų ruožus ir telefono numerius, atitinkamą (-us) sektorių (-ius) ir pasektorį (-ius), nurodytus I ir II prieduose. Subjektai turėtų pranešti kompetentingoms institucijoms apie visus tos informacijos pasikeitimus. Valstybės narės turėtų nepagrįstai nedelsdamos užtikrinti, kad tą informaciją būtų galima lengvai pateikti per vieno langelio principu veikiantį kontaktinį centrą. Tuo tikslu ENISA, bendradarbiaudama su Bendradarbiavimo grupe, turėtų nepagrįstai nedelsdama paskelbti gaires ir šablonus, susijusius su įpareigojimais teikti pranešimus. Valstybės narės turėtų pranešti Komisijai ir Bendradarbiavimo grupei apie esminių ir svarbių subjektų skaičių. Šioje direktyvoje nurodytos peržiūros tikslais valstybės narės taip pat turėtų pranešti Komisijai mažųjų ir labai mažų įmonių, kurios laikomi esminiais ir svarbiais subjektais, pavadinimus, kad Komisija galėtų įvertinti, ar valstybių narių metodai dera tarpusavyje. Ta informacija turėtų būti tvarkoma kaip griežtai konfidenciali;

Pakeitimas 11

Pasiūlymas dėl direktyvos
10 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(10) Komisija, bendradarbiaudama su Bendradarbiavimo grupe, ***gali*** paskelbti labai mažoms ir mažosioms įmonėms taikomų kriterijų įgyvendinimo gaires;	(10) Komisija, bendradarbiaudama su Bendradarbiavimo grupe ***ir atitinkamomis suinteresuotosiomis šalimis***, ***turėtų*** paskelbti labai mažoms ir mažosioms įmonėms taikomų kriterijų įgyvendinimo gaires***. Komisija taip pat turėtų užtikrinti, kad visoms labai mažoms ir mažosioms įmonėms, kurioms taikoma ši direktyva, būtų pateiktos tinkamos rekomendacijos. Komisija, padedama valstybių narių, turėtų suteikti labai mažoms ir mažosioms įmonėms informaciją tuo klausimu;***

Pakeitimas 12

Pasiūlymas dėl direktyvos
10 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(10a) Komisija taip pat turėtų parengti gaires, skirtas padėti valstybėms narėms tinkamai įgyvendinti nuostatas dėl taikymo srities ir įvertinti šioje direktyvoje nustatytų įpareigojimų proporcingumą, visų pirma atsižvelgiant į subjektus, kurių verslo modeliai arba veiklos aplinka yra sudėtingi, kadangi subjektas vienu metu gali atitikti ir esminiams, ir svarbiems subjektams nustatytus kriterijus arba tuo pat metu vykdyti veiklą, kurios dalis patenka į šios direktyvos taikymo sritį, o dalis nepatenka;

Pakeitimas 13

Pasiūlymas dėl direktyvos
12 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(12) konkrečių sektorių teisės aktai ir priemonės gali padėti užtikrinti aukšto lygmens kibernetinį saugumą kartu visapusiškai atsižvelgiant į šių sektorių specifiką ir sudėtingumą. ***Konkrečių sektorių Sąjungos teisės aktai, dėl kurių esminiai ir svarbūs subjektai turi priimti kibernetinio saugumo rizikos valdymo priemones arba pranešti apie reikšmingus incidentus, kai įmanoma, turėtų atitikti šioje direktyvoje nustatytą terminiją ir juose turėtų būti pateikiamos nuorodos į joje pateiktas apibrėžtis.*** Jeigu pagal konkrečiam sektoriui taikomą Sąjungos teisės aktą reikalaujama, kad esminiai arba svarbūs subjektai priimtų kibernetinio saugumo rizikos valdymo priemones arba praneštų apie incidentus, ir ***kai tie*** reikalavimai bent jau turi lygiavertį poveikį kaip ir šioje direktyvoje nustatytos pareigos ***ir taikomi visiems esminių ir svarbių***

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;

subjektų teikiamų operacijų ir paslaugų saugumo aspektams, turėtų būti taikomos tos konkretaus sektoriaus nuostatos, įskaitant priežiūrą ir vykdymo užtikrinimą reglamentuojančias nuostatas. Komisija ***turėtų*** priimti ***išsamias*** gaires, susijusias su lex specialis nuostatos įgyvendinimu***, atsižvelgdama į atitinkamas ENISA ir Bendradarbiavimo grupės nuomones, ekspertines žinias ir geriausią patirtį***. Šia direktyva nedraudžiama priimti papildomų konkretiems sektoriams taikomų Sąjungos aktų, kuriais reglamentuojamos kibernetinio saugumo rizikos valdymo priemonės ir pranešimo apie incidentus tvarka ***ir kuriais tinkamai atsižvelgiama į poreikį sukurti visa apimančią ir nuoseklią kibernetinio saugumo sistemą***. Ši direktyva nedaro poveikio dabartiniams įgyvendinimo įgaliojimams, kurie Komisijai suteikti įvairiuose sektoriuose, įskaitant transporto ir energetikos sektorius;

Pakeitimas 14

Pasiūlymas dėl direktyvos
14 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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 pagal Direktyvą (ES) XXX/XXX ***kompetentingos institucijos*** veikla dalijantis informacija apie incidentus bei	(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 pagal Direktyvą (ES) XXX/XXX ***kompetentingų institucijų*** veikla ***valstybėse narėse ir tarp valstybių narių***

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;

dalijantis informacija apie incidentus bei kibernetines grėsmes ir vykdant priežiūros užduotis. Institucijos pagal abi direktyvas turėtų bendradarbiauti ir keistis informacija ***nepagrįstai nedelsdamos***, 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 ***tikruoju laiku, kur tai įmanoma***;

---

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

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

Pakeitimas 15

Pasiūlymas dėl direktyvos
15 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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***	(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 ***aukščiausio lygio domenų (TLD) vardų serveriams***, ***viešai prieinamoms rekursinio domenų vardų keitimo paslaugoms galutiniams interneto naudotojams ir*** patikimo domenų vardų ***keitimo paslaugoms. Ši direktyva netaikoma šakninio pavadinimo***

keitiklius;	***serveriams***;

Pakeitimas 16

Pasiūlymas dėl direktyvos
19 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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***, atsižvelgiant į jų priklausomumo nuo tinklo ir informacinių sistemų laipsnį***. Teikiamos vežimo paslaugos, kai jos nėra susijusios su vienu iš šių etapų, neturėtų patekti į pašto paslaugų apibrėžtį;
[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).	[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).

Pakeitimas 17

Pasiūlymas dėl direktyvos
20 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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;

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 ***pandemijos metu padažnėję išpuoliai prieš tinklus ir informacines sistemas*** parodė, kad mūsų vis labiau tarpusavyje priklausoma visuomenė yra pažeidžiama atsižvelgiant į mažai tikėtiną riziką;

Pakeitimas 18

Pasiūlymas dėl direktyvos
24 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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 ***pagal šią direktyvą paskirti vieną ar daugiau*** CSIRT ***ir užtikrinti, kad jos gerai veiktų ir atitiktų*** esminius reikalavimus, kad būtų garantuoti veiksmingi bei suderinami incidentų bei rizikos valdymo pajėgumai ir užtikrintas veiksmingas bendradarbiavimas Sąjungos lygmeniu***. Valstybės narės gali CSIRT paskirti jau esamas kompiuterinių incidentų tyrimo***

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;	***tarnybas (CERT).*** 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;

Pakeitimas 19

Pasiūlymas dėl direktyvos
25 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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 ***arba kilus rimtai grėsmei nacionaliniam saugumui*** 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;
[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).	[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).

Pakeitimas 20

Pasiūlymas dėl direktyvos
25 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(25a) CSIRT turėtų gebėti subjekto prašymu nuolat nustatyti, valdyti ir stebėti visus su internetu susietus išteklius tiek patalpose, tiek debesijoje, kad suprastų jų bendrą organizacinę riziką, susijusią su naujai nustatytais tiekimo grandinės trūkumais ar ypatingos svarbos pažeidžiamumo aspektais. Žinojimas, ar subjektas naudoja privilegijuoto valdymo sąsają, daro poveikį švelninimo veiksmų įgyvendinimo spartai;

Pakeitimas 21

Pasiūlymas dėl direktyvos
26 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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***, taip pat su trečiųjų šalių CSIRT, jei keitimasis informacija yra abipusis ir naudingas piliečių ir įstaigų saugumui, kad galėtų prisidėti prie Sąjungos standartų, kurie gali formuoti kibernetinio saugumo aplinką tarptautiniu lygmeniu, rengimo. Valstybės narės taip pat galėtų išnagrinėti galimybę stiprinti bendradarbiavimą su panašių pažiūrų šalimis partnerėmis ir tarptautinėmis organizacijomis, siekiant užtikrinti daugiašalius susitarimus dėl kibernetinių normų, atsakingą valstybinių ir nevalstybinių subjektų elgesį kibernetinėje erdvėje ir veiksmingą pasaulinį skaitmeninį valdymą, taip pat sukurti atvirą, laisvą, stabilią ir saugią kibernetinę erdvę, grindžiamą tarptautine teise;***

Pakeitimas 22

Pasiūlymas dėl direktyvos
26 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(26a) kibernetinės higienos politikoje numatomi tinklų ir informacinių sistemų infrastruktūros, aparatinės įrangos, programinės įrangos ir internetinių programų, taip pat subjektų naudojamų verslo ir galutinių naudotojų duomenų apsaugos pagrindai. Kibernetinės higienos politika, kurioje pateikiamas su programinės ir aparatinės įrangos atnaujinimu, slaptažodžių keitimu, naujai įdiegtų programų valdymu, administratoriaus lygmens prieigos paskyrų ribojimu ir duomenų atsarginiu kopijavimu (bet ne tik su tuo) susijusios patirties pavyzdžių bendras pagrindinis rinkinys, sudaro aktyvią pasirengimo ir bendros saugos bei saugumo incidentų ar grėsmių atveju sistemą. ENISA turėtų stebėti ir vertinti valstybių narių kibernetinės higienos politiką ir svarstyti galimybę kurti Sąjungos masto sistemas, kad būtų galima atlikti tarpvalstybines patikras užtikrinant lygiavertiškumą, nepriklausomai nuo valstybių narių reikalavimų;

Pakeitimas 23

Pasiūlymas dėl direktyvos
26 b konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	***(26b) dirbtinio intelekto (DI) naudojimas kibernetinio saugumo srityje gali patobulinti išpuolių prieš tinklus ir informacines sistemas nustatymą ir juos sustabdyti, o išteklius būtų galima nukreipti į sudėtingesnius išpuolius. Todėl valstybės narės savo nacionalinėse**

	strategijose turėtų skatinti naudoti automatines priemones kibernetinio saugumo srityje ir dalytis duomenimis, kurių reikia (pusiau) automatizuotoms priemonės kibernetinio saugumo srityje apmokyti ir patobulinti. Siekiant sumažinti neteisėto asmenų teisių ir laisvių apribojimo, kurį gali kelti dirbtiniu intelektu grindžiamos sistemos, riziką, taikomi pritaikytosios ir standartizuotosios duomenų apsaugos reikalavimai, nustatyti Reglamento (ES) 2016/679 25 straipsnyje. Tokią riziką galėtų dar sumažinti tinkamų apsaugos priemonių, pavyzdžiui, pseudonimų suteikimo, šifravimo, duomenų tikslumo ir duomenų kiekio mažinimo, integravimas;

Pakeitimas 24

Pasiūlymas dėl direktyvos
26 c konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(26c) atvirojo kodo kibernetinio saugumo priemonėmis ir taikomosiomis programomis gali būti prisidedama prie didesnio skaidrumo ir daromas teigiamas poveikis pramonės inovacijų veiksmingumui. Atviraisiais standartais sudaromos sąlygos saugumo priemonių sąveikumui, o tai naudinga pramonės suinteresuotųjų subjektų saugumui. Atvirojo kodo kibernetinio saugumo priemonėmis ir taikomosiomis programomis gali būti daromas sverto poveikis platesnei programinės įrangos kūrėjų bendruomenei, sudarant subjektams galimybes vykdyti pardavėjų diversifikaciją ir atviras saugumo strategijas. Atvirasis saugumas gali paskatinti skaidresnį su kibernetiniu saugumu susijusių priemonių tikrinimo procesą ir bendruomenės inicijuotą pažeidžiamumų nustatymo procesą. Todėl valstybės narės turėtų skatinti atvirojo kodo programinės įrangos ir atvirųjų standartų diegimą, vykdydamos politiką,

	susijusią su atvirųjų duomenų ir atvirojo kodo naudojimu, kad skaidrumu būtų prisidėta prie saugumo užtikrinimo. Atvirojo kodo kibernetinio saugumo priemonių diegimo ir tvaraus naudojimo skatinimo politika itin svarbi mažosioms ir vidutinėms įmonėms (MVĮ), patiriančioms dideles įgyvendinimo sąnaudas, kurias galima būtų minimizuoti sumažinant poreikį naudoti konkrečias taikomąsias programas ar priemones;

Pakeitimas 25

Pasiūlymas dėl direktyvos
26 d konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(26d) viešojo ir privačiojo sektorių partnerystė kibernetinio saugumo srityje gali būti tinkama keitimosi žiniomis, dalijimosi geriausios patirties pavyzdžiais ir bendro supratimo tarp visų suinteresuotųjų subjektų nustatymo sistema. savo nacionalinėse kibernetinio saugumo strategijose valstybės narės turėtų priimti politiką, pagal kurią būtų kuriamos konkrečiai su kibernetiniu saugumu susijusios viešojo ir privačiojo sektorių partnerystės. Tokioje politikoje, be kita ko, turėtų būti patikslinama taikymo sritis ir dalyvaujantys suinteresuotieji subjektai, valdymo modelis, turimos finansavimo galimybės ir dalyvaujančių suinteresuotųjų subjektų tarpusavio ryšys. Viešojo ir privačiojo sektorių partnerystės gali naudotis privačiojo sektoriaus subjektų ekspertinėmis žiniomis, kad padėtų valstybių narių kompetentingoms institucijoms kurti pažangiausias paslaugas ir procesus, įskaitant keitimąsi informaciją, ankstyvąjį perspėjimą, kibernetinių grėsmių ir incidentų pratybas, krizių valdymą ir atsparumo planavimą, bet tuo neapsiribojant;

Pakeitimas 26

Pasiūlymas dėl direktyvos
27 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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 agentūros turėtų bendradarbiauti techniniu, operatyviniu ir politiniu lygmenimis, kad tinkamai koordinuotų atsaką visoje Sąjungoje;	(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***, arba kelti rimtą pavojų visuomenės saugumui ir piliečių bei subjektų saugai keliose valstybėse narėse arba visoje Sąjungoje***. Atsižvelgiant į tai, kad tokie incidentai yra labai įvairaus masto ir dažniausiai tarpvalstybinio pobūdžio, valstybės narės ir atitinkamos ES institucijos, įstaigos ir agentūros turėtų bendradarbiauti techniniu, operatyviniu ir politiniu lygmenimis, kad tinkamai koordinuotų atsaką visoje Sąjungoje;
[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).	[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).

Pakeitimas 27

Pasiūlymas dėl direktyvos
27 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(27a) savo nacionalinėse kibernetinio saugumo strategijose valstybės narės turėtų atsižvelgti į konkrečius MVĮ

	kibernetinio saugumo poreikius. Sąjungos kontekste MVĮ sudaro didelę pramoninės ir verslo rinkos procentinę dalį ir dažnai joms sunku prisitaikyti prie naujos verslo praktikos labiau susietame pasaulyje, kai naršoma skaitmeninė aplinka, o darbuotojai dirba iš namų ir verslas vis dažniau vyksta internetu. Kai kurios MVĮ susiduria su konkrečiomis kibernetinio saugumo problemomis, pvz., mažu informuotumu apie kibernetinį saugumą, nuotoliniu būdu administruojamo IT saugumo trūkumu, didelėmis kibernetinio saugumo sprendimų sąnaudomis ir padidėjusia grėsme, pvz., užkodavimo programomis, kurioms jos turėtų gauti gaires ir paramą. Valstybės narės turėtų turėti bendrąjį kibernetinio saugumo informacinį centrą, skirtą MVĮ, kuris teiktų MVĮ gaires ir paramą arba nukreiptų jas pas atitinkamus subjektus dėl rekomendacijų ir paramos kibernetinio saugumo klausimais. Valstybės narės raginamos taip pat teikti tokias paslaugas, kaip interneto svetainių konfigūravimas ir registravimas, kad jomis galėtų naudotis tokių gebėjimų neturinčios mažosios ir labai mažos įmonės;

Pakeitimas 28

Pasiūlymas dėl direktyvos
27 b konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(27b) valstybės narės turėtų priimti aktyvios kibernetinės gynybos skatinimo politiką, kaip savo nacionalinių kibernetinio saugumo strategijų dalį. Aktyvi kibernetinė gynyba yra aktyvi tinklo saugumo pažeidimų prevencija, aptikimas, stebėjimas, analizė ir poveikio švelninimas, kartu naudojant aukų tinkle ir kitur įdiegtus pajėgumus. Gebėjimas greitai ir automatiškai dalytis informacija apie grėsmes ir analize, įspėjimais apie kibernetinę veiklą ir informacija apie

reagavimo veiksmus ir juos suprasti yra labai svarbus siekiant užtikrinti, kad būtų imamasi vieningų pastangų sėkmingai aptikti išpuolius prieš tinklus ir informacines sistemas, užkirsti jiems kelią ir kovoti su jais. Aktyvi kibernetinė gynyba grindžiama gynybos strategija, pagal kurią neįtraukiamos prieš ypatingos svarbos civilinę infrastruktūrą nukreiptos puolamosios priemonės;

Pakeitimas 29

Pasiūlymas dėl direktyvos
28 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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. ***Norint sudaryti palankesnes sąlygas savanoriškai*** pažeidžiamumų ***atskleidimo sistemai***, ***labai svarbu stiprinti koordinavimą tarp*** pranešančiųjų subjektų ir IRT produktų ar paslaugų gamintojų ***ar*** teikėjų. 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

trečiosioms šalims arba visuomenei. Suderintas pažeidžiamumų atskleidimas taip pat turėtų apimti pranešančiojo subjekto ir organizacijos koordinavimą atsižvelgiant į taisymo laiką ir paskelbimą apie pažeidžiamumus;	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;

Pakeitimas 30

Pasiūlymas dėl direktyvos
28 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(28a) Komisija, ENISA ir valstybės narės turėtų tęsti tarptautinį derinimą su rizikos valdymo standartais ir dabartine pramonės sektoriaus gerąją patirtimi rizikos valdymo srityje, pavyzdžiui, tiekimo grandinės saugumo vertinimų, dalijimosi informacija ir pažeidžiamumų atskleidimo srityse;

Pakeitimas 31

Pasiūlymas dėl direktyvos
29 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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***	(29) todėl valstybės narės***, bendradarbiaudamos su ENISA,*** turėtų imtis priemonių ir nustatyti atitinkamą nacionalinę politiką, kad palengvintų suderintą pažeidžiamumų atskleidimą. ***Pagal šią nacionalinę politiką*** valstybės narės turėtų ***spręsti problemas***, ***su kuriomis susiduria pažeidžiamumų tyrėjai***. ***Kai kuriose valstybėse narėse pažeidžiamumus tiriantiems fiziniams asmenims*** ir ***subjektams gali grėsti baudžiamoji*** ir ***civilinė atsakomybė***. ***Todėl valstybės narės raginamos parengti gaires, kad dėl informacinio saugumo srities tyrimų nebūtų patraukiama baudžiamojon atsakomybėn ir nebūtų taikoma civilinė atsakomybė už šią veiklą***;

(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;

Pakeitimas 32

Pasiūlymas dėl direktyvos
29 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(29a) valstybės narės turėtų paskirti CSIRT, kad ji imtųsi koordinatorės vaidmens ir prireikus veiktų kaip tarpininkė tarp pranešančiųjų subjektų ir IRT produktų arba paslaugų gamintojų ar teikėjų, kuriems gali daryti poveikį pažeidžiamumas. 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;

Pakeitimas 33

Pasiūlymas dėl direktyvos
30 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(30) prieiga prie teisingos ir laiku pateikiamos informacijos apie pažeidžiamumus, kurie daro poveikį IRT produktams ir paslaugoms, padeda geriau valdyti kibernetinio saugumo riziką. Viešai prieinamos informacijos apie pažeidžiamumus šaltiniai yra svarbi ***priemonė*** ne tik ***subjektams*** ir jų ***naudotojams***, bet ir ***nacionalinėms kompetentingoms institucijoms*** bei CSIRT. Dėl šios priežasties ENISA turėtų sukurti pažeidžiamumų ***duomenų bazę***, ***kurioje*** 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***. Šios duomenų bazės tikslas – spręsti unikalias problemas, kylančias dėl kibernetinio saugumo rizikos, kylančios Europos subjektams. Be to, ENISA turėtų nustatyti patikimą procedūrą, susijusią su paskelbimo procesu, kad subjektai turėtų laiko imtis rizikos mažinimo priemonių, susijusių su jų pažeidžiamumais, ir naudotų naujausias kibernetinio saugumo priemones, taip pat kompiuterio skaitomus duomenų rinkinius ir atitinkamas sąsajas (API). Siekiant skatinti pažeidžiamumų atskleidimo kultūrą savanoriškas atskleidimas neturėtų pakenkti pranešančiajam subjektui;***

Pakeitimas 34

Pasiūlymas dėl direktyvos
31 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(31) ***nors panašūs pažeidžiamumų registrai arba duomenų bazės jau yra sukurti, jų prieglobą vykdo ir juos tvarko***	(31) ***ENISA tvarkomoje Europos pažeidžiamumo*** duomenų ***bazėje turėtų būti naudojamasi Bendro pažeidžiamumo***

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***;

ir ***rizikos (CVE) registru***, ***naudojant jo*** pažeidžiamumų ***nustatymo, sekimo*** ir ***vertinimo sistemą***. ***Be to***, ENISA turėtų išnagrinėti galimybę sudaryti struktūrinio bendradarbiavimo susitarimus su ***kitais*** panašiais registrais***, priklausančiais*** trečiųjų šalių ***jurisdikcijai, siekdama išvengti veiksmų dubliavimo ir siekti papildomumo***;

Pakeitimas 35

Pasiūlymas dėl direktyvos
33 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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, ***visų pirma dėl šios direktyvos perkėlimo į nacionalinę teisę suderinimo tarp valstybių narių palengvinimo,*** į kurias turėtų būti atsižvelgiama geriau įgyvendinant dabartines taisykles***. Bendradarbiavimo grupė taip pat turėtų apibendrinti nacionalinius sprendimus, kad būtų skatinamas kibernetinio saugumo sprendimų, taikomų kiekvienam konkrečiam sektoriui visoje Sąjungoje, suderinamumas. Tai ypač svarbu tarptautinio ir tarpvalstybinio pobūdžio sektoriams;***

Pakeitimas 36

Pasiūlymas dėl direktyvos
34 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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);	(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 ***atitinkamas*** kibernetinio saugumo politiką įgyvendinančias Sąjungos įstaigas ir agentūras, pavyzdžiui, ***Europolą***, Europos Sąjungos aviacijos saugos agentūrą (EASA) ir Europos Sąjungos kosmoso programos agentūrą (EUSPA);

Pakeitimas 37

Pasiūlymas dėl direktyvos
35 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(35) kompetentingoms institucijoms ir CSIRT turėtų būti suteikti įgaliojimai dalyvauti pareigūnų iš kitų valstybių narių mainų programose***, laikantis struktūruotų taisyklių ir mechanizmų, lemiančių taikymo sritį ir, kai taikytina, užtikrinančių reikiamą tokiose mainų programose dalyvaujančių pareigūnų patikimumo patikrinimą,*** siekiant pagerinti bendradarbiavimą ***ir didinti valstybių narių tarpusavio pasitikėjimą***. Kompetentingos institucijos turėtų imtis būtinų priemonių, kad pareigūnai iš kitų valstybių narių galėtų veiksmingai dalyvauti priimančiosios kompetentingos institucijos ***arba CSIRT*** veikloje;

Pakeitimas 38

Pasiūlymas dėl direktyvos
36 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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 ***užtikrinami Sąjungos interesai ir*** tinkama duomenų apsauga***. Tai nedaro poveikio valstybių narių teisei bendradarbiauti su bendramintėmis trečiosiomis šalimis valdant pažeidžiamumus ir kibernetinio saugumo riziką, palengvinant ataskaitų teikimą ir dalijimąsi bendraja informacija pagal Sąjungos teisę;***

Pakeitimas 39

Pasiūlymas dėl direktyvos
38 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	***Išbraukta.***

Pakeitimas 40

Pasiūlymas dėl direktyvos
39 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(39) šioje direktyvoje sąvoka „vos	***Išbraukta.***

neįvykę incidentai“ turėtų reikšti įvykį, kuris galėjo sukelti potencialią žalą, tačiau faktiniam jo atsitikimui buvo sėkmingai užkirstas kelias;

Pakeitimas 41

Pasiūlymas dėl direktyvos
40 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(40) rizikos valdymo priemonės turėtų apimti priemones, skirtas incidentų rizikai nustatyti, incidentų prevencijos, nustatymo, ***reagavimo į juos bei atsigavimo po jų*** ir jų poveikio švelninimo priemones. Tinklų ir informacinių sistemų saugumas turėtų apimti saugomų, perduodamų ir tvarkomų duomenų saugumą; ***Tokiose sistemose turėtų būti numatyta sisteminė analizė, atskirai analizuojant įvairius procesus ir posistemių sąveiką bei atsižvelgiant į žmogiškąjį faktorių, kad susidarytų visapusiškas informacinės sistemos saugumo vaizdas;***

Pakeitimas 42

Pasiūlymas dėl direktyvos
41 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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 ***ir Europos bei tarptautinius standartus, tokius kaip ISO31000 ir ISA/IEC 27005***;

Pakeitimas 43

Pasiūlymas dėl direktyvos
43 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(43) ***kibernetiniam saugumui kylančios*** rizikos subjekto tiekimo grandinėje ir subjekto ***santykiuose*** su ***tiekėjais, pavyzdžiui, duomenų saugojimo ir tvarkymo paslaugų teikėjais arba valdomų saugumo paslaugų teikėjais, šalinimas*** yra ypač ***svarbus*** atsižvelgiant į incidentų paplitimą tais atvejais, kai subjektai tapo ***atakų prieš tinklus ir informacines sistemas*** aukomis ir kai piktavališki dalyviai galėjo pažeisti subjekto tinklų ir informacinių sistemų saugumą pasinaudodami pažeidžiamumais, ***susijusiais su*** trečiųjų šalių ***produktais*** ir ***paslaugomis***. Todėl subjektai turėtų įvertinti ir atsižvelgti į bendrą savo tiekėjų ir paslaugų teikėjų produktų***, paslaugų*** ir ***juose integruotų kibernetinio saugumo priemonių ir*** kibernetinio saugumo praktikos, įskaitant jų saugaus tobulinimo procedūras, kokybę ***ir atsparumą. Subjektai visų pirma turėtų būti skatinami įtraukti kibernetinio saugumo priemones į susitarimus su pirmojo lygmens tiekėjais ir paslaugų teikėjais. Subjektai galėtų atsižvelgti į kibernetinio saugumo riziką, kylančią dėl kitų lygmenų tiekėjų ir paslaugų teikėjų;***

Pakeitimas 44

Pasiūlymas dėl direktyvos
44 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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 ***užkirsti kelią incidentams, juos nustatyti,*** į juos reaguoti

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;	***ir po jų atsigauti***. 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;

Pakeitimas 45

Pasiūlymas dėl direktyvos
45 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(45) subjektai taip pat turėtų mažinti kibernetinio saugumo riziką, kylančią dėl jų sąveikos ir santykių su kitomis suinteresuotosiomis šalimis platesnėje ekosistemoje***, be kita ko, siekiant kovoti su pramoniniu šnipinėjimu ir apsaugoti komercines paslaptis***. 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;

Pakeitimas 46

Pasiūlymas dėl direktyvos
45 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(45a) subjektai turėtų naudoti platų pagrindinių kompiuterio higienos praktikų, tokių kaip nulinio pasitikėjimo architektūra, programinės įrangos atnaujinimai, prietaisų konfigūravimas,

	tinklo segmentavimas, tapatybės ir prieigos valdymas arba naudotojų informuotumas, spektrą ir rengti darbuotojams mokymus apie įmonių e. pašto kibernetines grėsmes, duomenų vagystes ar socialinės inžinerijos metodus. Be to, subjektai turėtų įvertinti savo kibernetinio saugumo pajėgumus ir prireikus siekti integruoti kibernetinio saugumo stiprinimo technologijas, grindžiamas dirbtiniu intelektu ar mašinų mokymosi sistemomis, kad jų pajėgumai būtų automatizuoti ir būtų apsaugotos tinklo architektūros;

Pakeitimas 47

Pasiūlymas dėl direktyvos
46 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(46) siekiant toliau mažinti pagrindinę tiekimo grandinės riziką ir padėti subjektams, veikiantiems 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 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 ***ir RIS*** paslaugos, sistemos ar produktai, atitinkamos grėsmės ir pažeidžiamumai***. Tokiuose rizikos vertinimuose turėtų būti nustatytos priemonės, rizikos mažinimo planai ir geriausia patirtis kovojant su kritinėmis priklausomybėmis, galimais visuotinį neveikimą sukeliančiais gedimo taškais, grėsmėmis, pažeidžiamumais ir kitais rizikos veiksniais, susijusiais su tiekimo grandine, ir turėtų būti ieškoma būdų, kaip toliau skatinti subjektus juos plačiau taikyti. Galimi netechniniai***

	rizikos veiksniai, kaip antai nederama trečiosios šalies įtaka tiekėjams ir paslaugų teikėjams, visų pirma alternatyvių valdymo modelių atveju, apima paslėptas pažeidžiamas vietas arba apėjimo būdus ir galimus sisteminius tiekimo sutrikimus, visų pirma technologinio susaistymo arba priklausomybės nuo tiekėjų atveju;
[21] 2019 m. kovo 26 d. Komisijos rekomendacija (ES) 2019/534 dėl 5G tinklų kibernetinio saugumo (OL L 88, 2019 3 29, p. 42).	[21] 2019 m. kovo 26 d. Komisijos rekomendacija (ES) 2019/534 dėl 5G tinklų kibernetinio saugumo (OL L 88, 2019 3 29, p. 42).

Pakeitimas 48

Pasiūlymas dėl direktyvos
47 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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 ***per visą jų***

IRT paslaugų, sistemų ar produktų atveju, jų galimą būsimą svarbą subjektų veiklai;	***gyvavimo ciklą*** ir v) atsirandančių IRT paslaugų, sistemų ar produktų atveju, jų galimą būsimą svarbą subjektų veiklai***. Be to, ypatingas dėmesys turėtų būti skiriamas IRT paslaugoms, sistemoms ar produktams, kuriems taikomi konkretūs trečiųjų šalių reikalavimai;***

Pakeitimas 49

Pasiūlymas dėl direktyvos
47 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(47a) Suinteresuotųjų subjektų kibernetinio saugumo sertifikavimo grupė, įsteigta pagal Europos Parlamento ir Tarybos reglamento (ES) 2019/881[1a] 22 straipsnį, turėtų pateikti nuomonę dėl konkrečių ypatingos svarbos IRT ir RIS paslaugų, sistemų ar produktų tiekimo grandinių saugumo rizikos vertinimų. Bendradarbiavimo grupė ir ENISA turėtų atsižvelgti į tą nuomonę;
	[1a] 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).

Pakeitimas 50

Pasiūlymas dėl direktyvos
50 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(50) atsižvelgiant į didėjančią su numeriu nesiejamo asmenų tarpusavio ryšio paslaugų svarbą, būtina užtikrinti,	(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;	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 ***tinklo saugumo*** 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***.*** ***Tačiau, kadangi išpuolių mastas vis didėja, su numeriu nesiejamo asmenų tarpusavio ryšio paslaugos, įskaitant socialinės žiniasklaidos žinučių programas, bet jomis neapsiribojant, tampa populiariais išpuolių vektoriais. Kenkėjai naudoja platformas bendrauti su aukomis ir jas pritraukti į atvirus pavojingus puslapius, tad padidėja incidentų, susijusių su asmens duomenų eksploatavimu ir atitinkamai informacinių sistemų saugumu, tikimybė;***

Pakeitimas 51

Pasiūlymas dėl direktyvos
51 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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 ***visuose*** viešuosiuose elektroninių ryšių tinkluose, pavyzdžiui, interneto magistralėse ar povandeniniuose ryšių kabeliuose, būtų

kibernetinio saugumo priemonės ir būtų pranešama apie su jomis susijusius incidentus;	įdiegtos tinkamos kibernetinio saugumo priemonės ir būtų pranešama apie su jomis susijusius ***svarbius*** incidentus***. Valstybės narės turėtų užtikrinti, kad būtų išlaikytas tų viešųjų elektroninių ryšių tinklų vientisumas ir prieinamumas, ir turėtų apsvarstyti galimybę juos apsaugoti nuo gyvybiškai svarbių saugumo interesų sabotažo ir šnipinėjimo. Valstybės narės turėtų aktyviai dalytis informacija apie incidentus, pavyzdžiui, su povandeniniais ryšių kabėliais;***

Pakeitimas 52

Pasiūlymas dėl direktyvos
52 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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. ***Tai*** 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 ***ir parengta lengvai suprantama kalba***;

Pakeitimas 53

Pasiūlymas dėl direktyvos
53 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(53) ***viešųjų*** elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai turėtų ***įgyvendinti pritaikytojo ir standartizuotojo saugumo priemones ir*** informuoti paslaugų gavėjus apie konkrečias ir dideles kibernetines

saugumui užtikrinti, pavyzdžiui, naudodami konkrečių rūšių programinę įrangą arba ***šifravimo*** technologijas;	grėsmes ir priemones, kurių jie gali imtis savo ***įtaisų ir*** ryšių saugumui užtikrinti, pavyzdžiui, naudodami konkrečių rūšių ***šifravimo*** programinę įrangą arba ***į duomenis orientuotas saugumo*** technologijas;

Pakeitimas 54

Pasiūlymas dėl direktyvos
54 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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***;	(54) siekiant užtikrinti elektroninių ryšių tinklų ir paslaugų saugumą, turėtų būti skatinama naudoti šifravimą ***ir kitas į duomenis orientuotas saugumo technologijas***, ***kaip antai konvertavimą į žetonus, segmentavimą, ribotą prieigą, žymėjimą, ženklinimą, griežtą tapatybės ir prieigos valdymą ir automatinius sprendimus dėl prieigos***, ir, kai būtina, ***jos*** turėtų būti ***privalomos*** 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. ***Tačiau dėl to neturėtų būti dedamos jokios pastangos susilpninti ištisinį šifravimą, kuris yra itin svarbi technologija veiksmingai duomenų apsaugai ir privatumui užtikrinti***;

Pakeitimas 55

Pasiūlymas dėl direktyvos
54 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(54a) siekiant užtikrinti saugumą ir užkirsti kelią piktnaudžiavimui ir

	manipuliavimui elektroninių ryšių tinklais ir paslaugomis, turėtų būti skatinama naudoti sąveikius saugaus maršruto parinkimo standartus, kad būtų užtikrintas maršruto parinkimo funkcijų vientisumas ir patikimumas visoje interneto tiekėjų ekosistemoje;

Pakeitimas 56

Pasiūlymas dėl direktyvos
54 b konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(54b) siekiant apsaugoti interneto funkcionalumą ir vientisumą ir sumažinti su DNS susijusias saugumo problemas, atitinkami suinteresuotieji subjektai, įskaitant Sąjungos įmones, interneto paslaugų teikėjus ir naršyklių pardavėjus, turėtų būti skatinami priimti DNS keitimo įvairinimo strategiją. Be to, valstybės narės turėtų skatinti kurti ir naudoti viešą ir saugų Europos DNS keitiklį;

Pakeitimas 57

Pasiūlymas dėl direktyvos
55 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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, o ***išsamią*** ataskaitą privalo pateikti ne vėliau kaip per

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***;

vieną mėnesį po ***pradinio*** pranešimo ***pateikimo***. ***Pradinio pranešimo apie incidentą pateikimo terminas neturėtų trukdyti subjektams pranešti apie incidentus anksčiau***, ***taigi subjektai turi galimybę prašyti CSIRT paramos greitai***, ***sudarant galimybė apriboti galimą incidento***, ***apie kurį pranešta***, ***plitimą***. ***CSIRT gali prašyti tarpinės ataskaitos apie svarbius padėties pasikeitimus***, ***kartu atsižvelgdamos į pranešančiojo subjekto*** reagavimo į incidentus ir ***taisomuosius veiksmus***;

Pakeitimas 58

Pasiūlymas dėl direktyvos
55 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(55a) reikšmingas incidentas gali turėti įtakos paslaugos konfidencialumui, vientisumui ar prieinamumui. Esminiai ir svarbūs subjektai turėtų CSIRT pranešti apie reikšmingus incidentus, kurie daro poveikį jų paslaugų prieinamumui, per 24 valandas nuo tada, kai sužinojo apie incidentą. Apie reikšmingus incidentus, kuriais pažeidžiamas jų paslaugų konfidencialumas ir vientisumas, jie turėtų pranešti CIRT per 72 valandas nuo tada, kai sužinojo apie incidentą.

	Incidentų suskirstymas pagal tipus grindžiamas ne incidento rimtumu, o tuo, kad pranešančiajam subjektui sunku įvertinti incidentą, jo reikšmingumu ir galimybe pranešti informaciją, kuri gali būti naudingą CSIRT. Pradiniame pranešime turėtų būti pateikta informacija, kurios būtinai reikia, kad CSIRT žinotų apie incidentą, o subjektas prireikus galėtų kreiptis pagalbos. 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 CSIRT atitinkamas subjektas gali nukrypti nuo pradiniam pranešimui ir išsamios ataskaitos pateikimui nustatytų terminų;

Pakeitimas 59

Pasiūlymas dėl direktyvos
59 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(59) siekiant užtikrinti DNS saugumą, stabilumą ir atsparumą, būtina turėti tikslias***, patikrintas*** ir išsamias domenų vardų registracijos duomenų (vadinamųjų WHOIS duomenų) bazes, o tai savo ruožtu prisideda prie aukšto bendro kibernetinio saugumo lygio Sąjungoje ***ir kovos su neteisėta veikla. Todėl turėtų būti reikalaujama, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai rinktų domenų vardų registracijos duomenis, į kuriuos turėtų būti įtrauktas bent užsiregistravusiųjų***

vardas, jų faktinis ir e. pašto adresas, taip pat telefono numeris. Praktiškai surinkti duomenys ne visada gali būti visiškai tikslūs, tačiau aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys domenų vardų registravimo paslaugas, turėtų patvirtinti ir įgyvendinti proporcingas procedūras, skirtas patikrinti, ar fiziniai ar juridiniai asmenys, prašantys domeno vardo arba turintys jo nuosavybės teisę, pateikė kontaktinius duomenis, kuriais galima su jais susisiekti, ir tikėtis, kad jie į juos atsakys. Tos tikrinimo procedūros pagal principą „padaryti viską, kas įmanoma“ turėtų atspindėti šiuo metu sektoriuje taikomą geriausią praktiką. Ta geriausia tikrinimo procedūrų praktika turėtų atspindėti elektroninio identifikavimo proceso pažangą. Aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai turėtų viešai paskelbti savo politiką ir procedūras, kad būtų užtikrintas domenų vardų registracijos duomenų vientisumas ir prieinamumas. Kai tvarkomi asmens duomenys, toks tvarkymas turi atitikti Sąjungos duomenų apsaugos teisės aktus;

Pakeitimas 60

Pasiūlymas dėl direktyvos
60 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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***	(60) ***Kibernetinio saugumo ir kovos su neteisėta veikla interneto ekosistemoje tikslais labai svarbu užtikrinti domeno vardo registracijos*** duomenų ***prieinamumą*** ir ***galimybę*** laiku su jais susipažinti ***teisėtą prieigą gauti norintiems asmenims. Taigi pagal Sąjungos duomenų apsaugos teisę aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys domenų vardų registravimo paslaugas, turėtų būti įpareigojami suteikti teisėtą prieigą prie konkrečių domenų vardų registracijos***

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;***

duomenų, įskaitant asmens duomenis. Teisėtą prieigą norintys gauti subjektai turėtų pateikti tinkamai pagrįstą prašymą dėl prieigos prie domenų vardų registracijos duomenų pagal Sąjungos arba nacionalinę teisę ir tai galėtų būti kompetentingos institucijos pagal Sąjungos ar nacionalinę teisę***, atsakingos už*** nusikalstamų veikų ***nusikalstamų veikų prevenciją***, ***tyrimą*** ar ***baudžiamąjį persekiojimą*** už jas, ***ir nacionalinės*** CERT ***arba*** CSIRT***. Valstybės narės turėtų užtikrinti, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai nepagrįstai nedelsdami ir bet kuriuo atveju per 72 val. atsakytų į teisėtų prieigos siekiančių subjektų prašymus atskleisti domenų vardų registracijos duomenis. Aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys domenų vardų registravimo paslaugas, turėtų nustatyti registracijos duomenų skelbimo ir atskleidimo politiką ir procedūras, įskaitant susitarimus dėl paslaugų lygio, skirtus tvarkyti teisėtų prieigos siekiančių subjektų prašymus suteikti prieigą. Prieigos procedūra taip pat gali apimti sąsajos, portalo ar kitų techninių priemonių 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;***

Pakeitimas 61

Pasiūlymas dėl direktyvos
61 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(61) siekiant užtikrinti tikslių ir išsamių domenų vardų registracijos duomenų prieinamumą, aukščiausio lygio domenų	***Išbraukta.***

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;

Pakeitimas 62

Pasiūlymas dėl direktyvos
62 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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***	(62) ***turėtų būti reikalaujama, kad aukščiausio*** lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai viešai ***skelbtų juridinių asmenų kaip registruotojų*** domenų vardų registracijos duomenis, ***kurie neapima asmens*** duomenų***. Reikia taikyti skirtingą tvarką fiziniams ir juridiniams asmenims***[25]. ***Juridinių asmenų atveju*** aukščiausio lygio domenų vardų registrai ir subjektai turėtų ***viešai paskelbti bent užsiregistravusiųjų pavadinimą***, ***jų faktinį*** ir ***e. pašto adresą***, ***taip pat telefono numerį.*** Turėtų ***būti reikalaujama***, ***kad juridinis asmuo pateiktų bendrą e. pašto adresą, kuris gali būti skelbiamas viešai***, ***arba duotų sutikimą***, kad būtų ***paskelbtas asmeninis e. pašto adresas. Juridinis asmuo turėtų galėti įrodyti tokį sutikimą aukščiausio lygio domenų vardų registrų ir subjektų***, ***teikiančių domenų vardų registravimo paslaugas, prašymu***;

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;

---

[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“.

---

[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“.

Pakeitimas 63

Pasiūlymas dėl direktyvos
63 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(63) visi esminiai ir svarbūs subjektai, kuriems taikoma ši direktyva, turėtų priklausyti valstybės narės, kurioje jie teikia savo paslaugas ***arba vykdo veiklą***, 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;

Pakeitimas 64

Pasiūlymas dėl direktyvos
64 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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 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;	(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 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 ***arba valstybėje narėje***, ***kurioje*** subjektas turi padalinį, kuriame dirba daugiausia darbuotojų Sąjungoje***, arba valstybėje narėje, kurioje vykdomos kibernetinio saugumo operacijos***. Jeigu paslaugas teikia įmonių grupė, pagrindinė kontroliuojančiosios įmonės buveinė turėtų būti laikoma pagrindine įmonių grupės buveine;

Pakeitimas 65

Pasiūlymas dėl direktyvos
65 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(65a) ENISA turėtų sukurti ir tvarkyti registrą su informacija apie esminius ir svarbius subjektus, kurie yra DNS paslaugų teikėjai, aukščiausio lygio domenų vardų registrai ir debesijos kompiuterijos paslaugų teikėjai, duomenų centrų paslaugos, turinio teikimo tinklai, internetinės prekyvietės, internetinės paieškos sistemos ir socialinių tinklų platformos. Šie esminiai ir svarbūs subjektai turėtų pateikti ENISA savo pavadinimus, adresus ir naujausius kontaktinius duomenis. Jie turėtų nedelsdami ir bet kuriuo atveju ne vėliau kaip per dvi savaites nuo pakeitimo įsigaliojimo dienos pranešti ENISA apie bet kokius pateiktos informacijos pakeitimus. ENISA turėtų perduoti informaciją atitinkamam bendrajam informaciniam centrui. Todėl esminiai ir svarbūs subjektai, teikiantys informaciją ENISA, neprivalo atskirai informuoti valstybės narės kompetentingą instituciją. ENISA turėtų sukurti paprastą viešai prieinamą taikomąją programą, kurią tie subjektai galėtų naudoti savo informacijai atnaujinti. Be to, ENISA turėtų nustatyti tinkamus informacijos klasifikavimo ir valdymo protokolus, kad užtikrintų atskleistos informacijos saugumą ir konfidencialumą, ir apriboti prieigą prie tokios informacijos, jos saugojimą ir perdavimą numatytiems naudotojams;

Pakeitimas 66

Pasiūlymas dėl direktyvos
66 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(66) jeigu pagal šios direktyvos	(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;	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***. Be to, ENISA turėtų turėti infrastruktūrą, procedūras ir taisykles, kuriomis būtų tvarkoma neskelbtina ir įslaptinta informacija, laikantis ES įslaptintai informacijai apsaugoti taikomų saugumo taisyklių;***

Pakeitimas 67

Pasiūlymas dėl direktyvos
68 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(68) subjektai turėtų***,*** skatinami ***ir remiami valstybių narių,*** 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***, kaip antai subjektus, sutelkiančius dėmesį į kibernetinio saugumo paslaugas ir mokslinius tyrimus***, dalyvauti tokiuose keitimosi informacija mechanizmuose. Tie mechanizmai turėtų būti taikomi visapusiškai laikantis Sąjungos konkurencijos taisyklių ir Sąjungos teisės nuostatų dėl duomenų apsaugos;

Pakeitimas 68

Pasiūlymas dėl direktyvos
69 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(69) ***esminių ir svarbių subjektų***, CSIRT ir saugumo technologijų bei paslaugų teikėjų vykdomas asmens duomenų tvarkymas tiek, kiek tai tikrai būtina ir proporcinga siekiant užtikrinti tinklų ir informacijos saugumą, ***yra būtinas, kad būtų laikomasi šioje direktyvoje numatytų teisinių įsipareigojimų. Toks asmens duomenų tvarkymas taip pat gali*** būti ***reikalingas siekiant teisėtų esminių ir svarbių subjektų interesų. Kai šioje direktyvoje reikalaujama asmens duomenis tvarkyti kibernetinio saugumo, tinklo ir informacijos saugumo tikslais pagal direktyvos 18, 20 ir 23 straipsnių nuostatas, laikoma***, ***jog duomenis tvarkyti yra teisiškai privaloma, laikantis Reglamento*** (ES) 2016/679 ***6 straipsnio 1 dalies c punkto***. ***Taikant šios direktyvos 26 ir 27 straipsnius, Reglamento (ES) 2016/679 6 straipsnio 1 dalies f punkte nurodytas tvarkymas laikomas būtinu siekiant teisėtų esminių ir svarbių subjektų interesų. Taikant*** priemones, susijusias su incidentų prevencija, nustatymu, ***identifikavimu, apribojimu,*** 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 ***reikia tvarkyti tam tikrų kategorijų*** asmens duomenis***, pvz.,*** IP adresus, universaliuosius išteklių adresus (URL), domenų vardus***,*** e. pašto adresus***, laiko žymas, su operacine sistema arba naršykles susijusią informaciją, slapukus arba kitą informaciją, iš kurios matyti modus operandi***;

Pakeitimas 69

Pasiūlymas dėl direktyvos
71 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(71) kad vykdymo užtikrinimas būtų veiksmingas, turėtų būti parengtas būtinas administracinių ***nuobaudų*** už šioje direktyvoje nustatytų kibernetinio saugumo rizikos valdymo ir pranešimo pareigų pažeidimą sąrašas, kuriuo būtų sukurta aiški ir nuosekli tokių ***nuobaudų*** sistema visoje Sąjungoje. Reikėtų deramai atsižvelgti į pažeidimo pobūdį, rimtumą ir trukmę, padarytą žalą ar patirtus nuostolius, 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. ***Nuobaudos***, įskaitant administracines baudas, turėtų būti ***proporcingos ir jas skiriant turėtų būti*** taikomos tinkamos procedūrinės apsaugos priemonės pagal bendruosius Sąjungos teisės principus ir Europos Sąjungos pagrindinių teisių chartiją ***(toliau – Chartija)***, įskaitant veiksmingą teisminę apsaugą***,*** tinkamą procesą***, nekaltumo prezumpciją ir teisę į gynybą***;

Pakeitimas 70

Pasiūlymas dėl direktyvos
72 konstatuojamoji dalis

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

skirti;	skirti***, jeigu pažeidimas buvo tyčinis ar dėl neapdairumo arba susijusiam subjektui buvo iš anksto pranešta apie subjekto pareigų nevykdymą***;

Pakeitimas 71

Pasiūlymas dėl direktyvos
76 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(76) siekiant dar labiau sustiprinti sankcijų, taikomų už pagal šią direktyvą nustatytų pareigų pažeidimus, veiksmingumą ir atgrasomumą, kompetentingoms institucijoms turėtų būti suteikti įgaliojimai ***laikinai sustabdyti sertifikavimą*** ar ***leidimą***, ***susijusį*** su dalies ar visų ***atitinkamų*** esminių subjektų teikiamų paslaugų teikimu, ir ***reikalauti laikinai uždrausti*** fiziniam asmeniui eiti ***generalinio direktoriaus arba teisinio atstovo lygmens*** vadovaujamas pareigas***. Valstybės narės turėtų parengti konkrečias procedūras ir taisykles, susijusias su laikinu draudimu fiziniam asmeniui eiti generalinio direktoriaus arba teisinio atstovo lygmens vadovaujamas pareigas viešojo administravimo subjektuose. Rengdamos tokias procedūras ir taisykles, valstybės narės turėtų atsižvelgti į savo viešojo administravimo atitinkamų lygmenų ir valdymo sistemų ypatumus.*** Atsižvelgiant į tokių ***laikinų sustabdymų ar draudimų*** 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. ***Tokie laikini sustabdymai ar draudimai*** turėtų būti ***taikomi*** tik kaip ultima ratio, t. y. tik po to, kai išnaudojami kiti šioje direktyvoje nustatyti atitinkami vykdymo užtikrinimo

teisę į gynybą;	veiksmai, ir tik tol, kol subjektai, kuriems jos taikomos, imasi reikiamų veiksmų trūkumams pašalinti arba kompetentingos institucijos, kuriai ***taikyti tokie laikini sustabdymai ar draudimai***, reikalavimams įvykdyti. Skiriant ***tokius laikinus sustabdymus ar draudimus***, turėtų būti taikomos tinkamos procedūrinės apsaugos priemonės pagal bendruosius Sąjungos teisės ***ir Chartijos*** principus, įskaitant veiksmingą teisminę apsaugą, tinkamą procesą, nekaltumo prezumpciją ir teisę į gynybą;

Pakeitimas 72

Pasiūlymas dėl direktyvos
79 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(79) turėtų būti nustatytas tarpusavio vertinimo mechanizmas, pagal kurį valstybių narių paskirti nepriklausomi ekspertai galėtų įvertinti, kaip įgyvendinama kibernetinio saugumo politika, įskaitant valstybių narių pajėgumų lygį ir turimus išteklius. ***Tarpusavio vertinimai gali padėti gauti vertingų įžvalgų ir rekomendacijų, kuriomis stiprinami bendri kibernetinio saugumo pajėgumai. Visų pirma jos gali padėti sudaryti palankesnes sąlygas tarpusavio vertinime dalyvaujančioms valstybėms narėms perduoti technologijas, įrankius, priemones ir procesus, sukurti funkcionalų būdą dalytis geriausia patirtimi valstybėms narėms, kurių kibernetinio saugumo brandos lygis yra skirtingas, ir sudaryti sąlygas visoje Sąjungoje užtikrinti aukštą bendrą kibernetinio saugumo lygį. Prieš atliekant tarpusavio vertinimą, vertinamoji valstybė narė turėtų atlikti savęs vertinimą, apimantį vertinamus aspektus ir visus papildomus tikslinius klausimus, apie kuriuos paskirti ekspertai praneša tarpusavio vertinime dalyvaujančiai valstybei narei prieš pradedant procesą.***

	Komisija, bendradarbiaudama su ENISA ir Bendradarbiavimo grupe, turėtų parengti vertinamų aspektų įsivertinimo šablonus, kad procesas būtų paprastesnis ir būtų išvengta procedūrinių nenuoseklumo ir vėlavimo. Tuos šablonus turėtų užpildyti valstybės narės, kurių tarpusavio vertinimas atliekamas, ir juos pateikti paskirtiems ekspertams, atliekantiems tarpusavio vertinimą prieš pradedant tarpusavio vertinimo procesą;

Pakeitimas 73

Pasiūlymas dėl direktyvos
80 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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 ***kibernetiniam saugumui kylančios*** rizikos valdymo priemonėmis ***ir pareigomis pranešti***, kurių reikalaujama pagal šią direktyvą. Komisijai taip pat turėtų būti suteikti įgaliojimai priimti deleguotuosius aktus, kuriais būtų nustatyta, kokių kategorijų esminiams ***ir svarbiems*** 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. 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

aktais susijusį parengiamąjį darbą, posėdžiuose;	Komisijos ekspertų grupių, kurios atlieka su deleguotaisiais aktais susijusį parengiamąjį darbą, posėdžiuose;

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

Pakeitimas 74

Pasiūlymas dėl direktyvos
81 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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];	(81) siekiant užtikrinti vienodas atitinkamų šios direktyvos nuostatų, susijusių su Bendradarbiavimo grupės veikimui būtina procedūrine tvarka, pranešimų apie incidentus 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];
[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).	[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).

Pakeitimas 75

Pasiūlymas dėl direktyvos
82 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(82) Komisija, konsultuodamasi su suinteresuotosiomis šalimis, turėtų periodiškai peržiūrėti šią direktyvą, visų pirma siekdama nustatyti, ar ***reikia ją keisti*** atsižvelgiant į kintančias visuomenines,	(82) Komisija, konsultuodamasi su suinteresuotosiomis šalimis, turėtų periodiškai peržiūrėti šią direktyvą, visų pirma siekdama nustatyti, ar ***tikslinga siūlyti pakeitimus*** atsižvelgiant į kintančias

politines, technologines ar rinkos sąlygas;	visuomenines, politines, technologines ar rinkos sąlygas***. Atlikdama minėtas peržiūras, Komisija turėtų įvertinti prieduose nurodytų sektorių, pasektorių ir subjektų tipų svarbą ekonomikos ir visuomenės veikimui kibernetinio saugumo atžvilgiu. Komisija turėtų, inter alia, įvertinti, ar skaitmeniniai paslaugų teikėjai, kurie pagal Reglamento (ES) XXXX/XXXX [Bendrosios skaitmeninių paslaugų rinkos aktas (Skaitmeninių paslaugų aktas)] 25 straipsnį priskiriami labai didelėms interneto platformoms arba prieigos valdytojams, kaip apibrėžta Reglamento (ES) XXXX/XXXX [Reglamentas dėl konkurencingų ir sąžiningų skaitmeninio sektoriaus rinkų (Skaitmeninių rinkų aktas)] 2 straipsnio 1 punkte, turėtų būti paskirti esminiais subjektais pagal šią direktyvą. Be to, Komisija turėtų įvertinti, ar tikslinga iš dalies pakeisti Europos Parlamento ir Tarybos direktyvos 2020/1828[1a] I priedą, įtraukiant nuorodą į šią direktyvą***; ***[1a] 2020 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2020/1828 dėl atstovaujamųjų ieškinių siekiant apsaugoti vartotojų kolektyvinius interesus, kuria panaikinama Direktyva 2009/22/EB (OL L 409, 2020 12 4, p. 1).***

Pakeitimas 76
Pasiūlymas dėl direktyvos
82 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(82a) šia direktyva nustatomi kibernetinio saugumo reikalavimai valstybėms narėms ir Sąjungoje įsteigtiems esminiams ir svarbiems subjektams. Tuos kibernetinio saugumo reikalavimus taip pat turėtų taikyti Sąjungos institucijos, įstaigos, tarnybos ir agentūros, remdamosi Sąjungos teisės aktu;

Pakeitimas 77

Pasiūlymas dėl direktyvos
82 b konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(82b) šia direktyva sukuriamos naujos ENISA užduotys ir taip sustiprinamas jos vaidmuo, o dėl to ENISA galėtų būti keliami reikalavimus vykdyti esamas užduotis pagal Reglamentą (ES) 2019/881 laikantis aukštesnių standartų nei anksčiau. Siekiant užtikrinti, kad ENISA turėtų reikiamų finansinių ir žmogiškųjų išteklių, kad galėtų vykdyti esamą ir naują veiklą pagal jos užduotis, taip pat atitikti aukštesnius standartus, susijusius su sustiprintu jos vaidmeniu, jos biudžetas turėtų būti atitinkamai padidintas. Be to, siekiant užtikrinti veiksmingą išteklių panaudojimą, ENISA turėtų būti suteikta daugiau lankstumo, kad jai būtų leidžiama skirstyti išteklius viduje, kad ji galėtų veiksmingai vykdyti savo užduotis ir patenkinti lūkesčius.

Pakeitimas 78

Pasiūlymas dėl direktyvos
84 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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**,**	(84) šia direktyva gerbiamos pagrindinės teisės ir laikomasi principų, pripažintų 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. ***Tai apima esminių ir svarbių subjektų teikiamų paslaugų gavėjų teisę į veiksmingą teisinę gynybą.*** Ši direktyva turėtų būti įgyvendinta atsižvelgiant į tas teises ir principus**.**

Pakeitimas 79

Pasiūlymas dėl direktyvos
1 straipsnio 2 dalies c a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ca) valstybių narių priežiūros ir vykdymo užtikrinimo pareigos.

Pakeitimas 80

Pasiūlymas dėl direktyvos
2 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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].	1. Ši direktyva taikoma ***esminiams ir svarbiems*** viešiesiems ir privatiesiems subjektams, kurie I priede įvardijami kaip esminiai subjektai, o II priede – kaip svarbūs subjektai***, teikiantys savo paslaugas arba vykdantys veiklą Sąjungoje***. Ši direktyva netaikoma labai ***mažoms*** ir ***mažosioms įmonėms, apibrėžtoms*** Komisijos ***rekomendacijos*** 2003/361/EB[28] ***priedo 2 straipsnio 2 ir 3 dalyse. Tos rekomendacijos priedo 3 straipsnio 4 dalis netaikoma.***
[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).	[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).

Pakeitimas 81

Pasiūlymas dėl direktyvos
2 straipsnio 2 dalies 1 pastraipos įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
Tačiau, nepaisant subjektų dydžio, ši direktyva taikoma ***I*** ir ***II prieduose nurodytiems*** subjektams, kai:	Nepaisant subjektų dydžio, ši direktyva ***taip pat*** taikoma ***esminiams*** ir ***svarbiems*** subjektams, kai:

Pakeitimas 82

Pasiūlymas dėl direktyvos
2 straipsnio 2 dalies 1 pastraipos d punktas

Komisijos siūlomas tekstas	*Pakeitimas*
d) ***potencialus*** paslaugos, kurią teikia subjektas, sutrikimas galėtų turėti poveikį viešajam saugumui, visuomenės saugumui arba visuomenės sveikatai;	d) paslaugos, kurią teikia subjektas, sutrikimas galėtų turėti poveikį viešajam saugumui, visuomenės saugumui arba visuomenės sveikatai;

Pakeitimas 83

Pasiūlymas dėl direktyvos
2 straipsnio 2 dalies 1 pastraipos e punktas

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

Pakeitimas 84

Pasiūlymas dėl direktyvos
2 straipsnio 2 dalies 2 pastraipa

Komisijos siūlomas tekstas	*Pakeitimas*
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.	***Išbraukta.***

Pakeitimas 85

Pasiūlymas dėl direktyvos
2 straipsnio 2 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	2a. Ne vėliau kaip ... [6 mėnesiai po perkėlimo į nacionalinę teisę termino] valstybės narės sudaro esminių ir svarbių subjektų, įskaitant 1 dalyje nurodytus subjektus ir pagal 2 dalies b-f punktus ir 24 straipsnio 1 dalį nustatytus subjektus, sąrašą. Valstybės narės nuolat ir ne rečiau kaip kas dvejus metus peržiūri sąrašą ir, kai tinkama, jį atnaujina.

Pakeitimas 86

Pasiūlymas dėl direktyvos
2 straipsnio 2 b dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	2b. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai kompetentingoms institucijoms pateiktų bent tokią informaciją:
	a) subjekto pavadinimą;
	b) naujausius kontaktinius duomenis, įskaitant subjektų e. pašto adresus, IP adresų ruožus ir telefonų numerius bei
	c) I ir II prieduose nurodytą (-us) atitinkamą (-us) sektorių (-ius) ir pasektorių (-ius).
	Esminiai ir svarbūs subjektai nedelsdami ir bet kuriuo atveju ne vėliau kaip per dvi savaites nuo pakeitimo įsigaliojimo dienos praneša apie bet kokius jų pagal pirmą pastraipą pateiktų duomenų pakeitimus. Tuo tikslu Komisija, padedama ENISA, nepagrįstai nedelsdama parengia gaires ir šablonus, susijusius su šioje dalyje nustatytomis pareigomis.

Pakeitimas 87

Pasiūlymas dėl direktyvos
2 straipsnio 2 c dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	2c. Ne vėliau kaip ... [6 mėnesiai po perkėlimo į nacionalinę teisę termino], o vėliau kas dvejus metus valstybės narės praneša:
	a) Komisijai ir Bendradarbiavimo grupei visų esminių ir svarbių subjektų, identifikuotų kiekvienam iš I ir II prieduose nurodytų sektorių ir pasektorių, skaičių;
	b) Komisijai pagal 2 dalies b-f punktus nustatytų subjektų pavadinimus.

Pakeitimas 88

Pasiūlymas dėl direktyvos
2 straipsnio 4 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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].	4. Ši direktyva taikoma nedarant poveikio Tarybos direktyvai 2008/114/EB[30] ir Europos Parlamento ir Tarybos direktyvoms 2011/93/ES[31]***,*** 2013/40/ES[32] ***ir 2002/58/EB[32a]***.
[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).	[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).	[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	[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).	informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (OL L 218, 2013 8 14, p. 8). ***[32a] 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).***

Pakeitimas 89

Pasiūlymas dėl direktyvos
2 straipsnio 6 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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, 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. ***Komisija nepagrįstai nedelsdama paskelbia gaires, susijusias su konkrečių sektorių Sąjungos teisės aktų įgyvendinimu, kad užtikrintų, kad tais aktais būtų įvykdomi šioje direktyvoje nustatyti kibernetinio saugumo reikalavimai ir kad nebūtų dubliavimosi ar teisinio netikrumo. Rengdama tas gaires Komisija atsižvelgia į ENISA ir Bendradarbiavimo grupės geriausią patirtį ir ekspertines žinias.***

Pakeitimas 90

Pasiūlymas dėl direktyvos
2 straipsnio 6 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	6a. Esminiai ir svarbūs subjektai, CSIRT ir saugumo technologijų bei paslaugų teikėjai, tvarko asmens duomenis tiek, kiek tai yra būtina ir proporcinga kibernetinio saugumo, tinklo ir informacijos saugumo sumetimais, kad įvykdytų šioje direktyvoje nustatytus įpareigojimus. Asmens duomenys pagal šią direktyvą tvarkomi laikantis Reglamento (ES) 2016/679, visų pirma jo 6 straipsnio.

Pakeitimas 91

Pasiūlymas dėl direktyvos
2 straipsnio 6 b dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	6b. Asmens duomenų tvarkymą pagal šią direktyvą viešųjų elektroninių ryšių tinklų paslaugų teikėjai arba I priedo 8 punkte nurodyti viešai prieinamų elektroninių ryšių paslaugų teikėjai vykdo laikantis Direktyvos 2002/58/EB.

Pakeitimas 92

Pasiūlymas dėl direktyvos
4 straipsnio 1 pastraipos 4 a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	4a) vos neįvykęs incidentas – įvykis, kuriuo galėjo būti pažeistas duomenų prieinamumas, autentiškumas, vientisumas arba konfidencialumas arba galėjo būti padaryta žala, tačiau kuriam buvo sėkmingai užkirstas kelias padaryti neigiamą poveikį;

Pakeitimas 93

Pasiūlymas dėl direktyvos
4 straipsnio 1 pastraipos 6 punktas

Komisijos siūlomas tekstas	*Pakeitimas*
6) incidento valdymas – visi veiksmai ir procedūros, kuriais siekiama nustatyti, išanalizuoti ir sustabdyti incidentą ir į jį reaguoti;	6) incidento valdymas – visi veiksmai ir procedūros, kuriais siekiama ***užkardyti,*** nustatyti, išanalizuoti ir sustabdyti incidentą ir į jį reaguoti;

Pakeitimas 94

Pasiūlymas dėl direktyvos
4 straipsnio 1 pastraipos 7 a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	7a) rizika – potencialus praradimas arba sutrikimas, kurį sukėlė incidentas, ir ji turėtų būti išreikšta kaip tokio praradimo arba sutrikimo masto ir to incidento pasikartojimo derinys;

Pakeitimas 95

Pasiūlymas dėl direktyvos
4 straipsnio 1 pastraipos 11 punktas

Komisijos siūlomas tekstas	*Pakeitimas*
11) techninė specifikacija – techninė specifikacija, kaip apibrėžta Reglamento (ES) Nr. ***1025/2012 4 straipsnio 2 dalyje***;	11) techninė specifikacija – techninė specifikacija, kaip apibrėžta Reglamento (ES) Nr. ***2019/881 2 straipsnio 20 punkte***;

Pakeitimas 96

Pasiūlymas dėl direktyvos
4 straipsnio 1 pastraipos 13 punktas

Komisijos siūlomas tekstas	*Pakeitimas*
13) domenų vardų sistema (DNS) – hierarchiškai paskirstyta vardų sistema, ***kuri sudaro sąlygas*** galutiniams naudotojams ***gauti paslaugas*** ir ***pasinaudoti interneto ištekliais***;	13) domenų vardų sistema (DNS) – hierarchiškai paskirstyta vardų sistema, ***kurioje galima identifikuoti interneto paslaugas ir išteklius ir sudaromos sąlygos*** galutiniams naudotojams ***naudotis interneto maršruto parinkimo ir junglumo***

	paslaugomis ir ***gauti tas paslaugas bei išteklius***;

Pakeitimas 97

Pasiūlymas dėl direktyvos
4 straipsnio 1 pastraipos 14 punktas

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

Pakeitimas 98

Pasiūlymas dėl direktyvos
4 straipsnio 1 pastraipos 14 punkto a papunktis (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	a) atviras ir viešąsias rekursinio domenų vardų keitimo paslaugas galutiniams interneto naudotojams arba

Pakeitimas 99

Pasiūlymas dėl direktyvos
4 straipsnio 1 pastraipos 14 punkto b papunktis (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	b) patikimo domenų vardų keitimo paslaugas, kaip trečiųjų šalių subjektų perkamą paslaugą;

Pakeitimas 100

Pasiūlymas dėl direktyvos
4 straipsnio 1 pastraipos 15 punktas

Komisijos siūlomas tekstas	*Pakeitimas*
15) aukščiausio lygio domenų vardų registras – subjektas, kuriam pavestas konkretus aukščiausio lygio domenas ir	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;	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***, neatsižvelgiant į tai, ar bet kurias iš tų operacijų atlieka subjektas, ar tai yra užsakomosios paslaugos***;

Pakeitimas 101

Pasiūlymas dėl direktyvos
4 straipsnio 1 pastraipos 15 a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	15a) domenų vardų registravimo paslaugos – paslaugos, kurias teikia domenų vardų registrai ir registratoriai, privatumo arba įgaliotojo serverio domenų vardų registravimo paslaugų teikėjai, domenų brokeriai ar perpardavėjai, ir visos kitos paslaugos, susijusios su domenų vardų registravimu;

Pakeitimas 102

Pasiūlymas dėl direktyvos
4 straipsnio 1 pastraipos 23 a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	23a) viešasis elektroninių ryšių tinklas – viešasis elektroninių ryšių tinklas, kaip apibrėžta Direktyvos (ES) 2018/1972 2 straipsnio 8 punkte;

Pakeitimas 103

Pasiūlymas dėl direktyvos
4 straipsnio 1 pastraipos 23 b punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	23b) elektroninių ryšių paslauga –

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

Pakeitimas 104

Pasiūlymas dėl direktyvos
5 straipsnio 1 dalies įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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:	1. Kiekviena valstybė narė priima nacionalinę kibernetinio saugumo strategiją, kurioje apibrėžiami strateginiai tikslai***, reikiami techniniai, organizaciniai ir finansiniai ištekliai tiems tikslams pasiekti*** ir tinkamos politikos bei reguliavimo priemonės, kad būtų pasiektas ir išlaikytas aukšto lygmens kibernetinis saugumas. Nacionalinėje kibernetinio saugumo strategijoje visų pirma pateikiama:

Pakeitimas 105

Pasiūlymas dėl direktyvos
5 straipsnio 1 dalies a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) ***valstybių narių*** kibernetinio saugumo strategijos tikslų ir prioritetų apibrėžtis;	a) ***valstybės narės*** kibernetinio saugumo strategijos tikslų ir prioritetų apibrėžtis;

Pakeitimas 106

Pasiūlymas dėl direktyvos
5 straipsnio 1 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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***;	b) valdymo sistema, kad būtų pasiekti tie tikslai ir įgyvendinti prioritetai, įskaitant 2 dalyje nurodytą politiką;

Pakeitimas 107

Pasiūlymas dėl direktyvos
5 straipsnio 1 dalies b a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ba) sistema, nustatanti viešųjų įstaigų ir subjektų, taip pat kitų susijusių subjektų vaidmenis ir pareigas, kuria nacionaliniu lygmeniu grindžiamas bendradarbiavimas ir koordinavimas tarp kompetentingų institucijų, paskirtų pagal 7 straipsnio 1 dalį ir 8 straipsnio 1 dalį, bendrojo informacinio centro, paskirto pagal 8 straipsnio 3 dalį, ir CSIRT, paskirtų pagal 9 straipsnį;

Pakeitimas 108

Pasiūlymas dėl direktyvos
5 straipsnio 1 dalies e punktas

Komisijos siūlomas tekstas	*Pakeitimas*
e) įvairių institucijų ir dalyvių, dalyvaujančių įgyvendinant nacionalinę kibernetinio saugumo strategiją, sąrašas;	e) įvairių institucijų ir dalyvių, dalyvaujančių įgyvendinant nacionalinę kibernetinio saugumo strategiją, sąrašas***, į kurį būtų įtrauktas bendrasis kibernetinio saugumo informacinis centras, kuris teikia paramą MVĮ įgyvendinant konkrečias kibernetinio saugumo priemones***;

Pakeitimas 109

Pasiūlymas dėl direktyvos
5 straipsnio 1 dalies f punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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	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 ***valstybėse narėse ir tarp jų*** siekiant dalytis informacija apie incidentus bei

užduotis.

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

kibernetines grėsmes ir vykdyti priežiūros užduotis.

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

Pakeitimas 110

Pasiūlymas dėl direktyvos
5 straipsnio 1 dalies f a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	fa) piliečių informuotumo apie kibernetinį saugumą bendro lygio vertinimas.

Pakeitimas 111

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies -a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	-a) kiekvieno sektoriaus, kuriam taikoma ši direktyva, politiką dėl kibernetinio saugumo klausimų;

Pakeitimas 112

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
b) gaires dėl su kibernetiniu saugumu susijusių reikalavimų, taikomų IRT produktams ir paslaugoms viešuosiuose pirkimuose, ir tokių reikalavimų specifikacijų;	b) gaires dėl su kibernetiniu saugumu susijusių reikalavimų, taikomų IRT produktams ir paslaugoms viešuosiuose pirkimuose, ir tokių reikalavimų specifikacijų***, įskaitant šifravimo reikalavimus ir atvirojo kodo kibernetinio saugumo produktų naudojimą***;

Pakeitimas 113

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies d punktas

Komisijos siūlomas tekstas	*Pakeitimas*
d) politiką, susijusią su bendru atvirojo interneto viešojo pagrindo prieinamumu ir vientisumu;	d) politiką, susijusią su bendru atvirojo interneto viešojo pagrindo prieinamumu ir vientisumu***, įskaitant interneto magistralių ir povandeninių ryšių kabelių kibernetinį saugumą***;

Pakeitimas 114

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies d a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	da) politiką, kuria skatinamas ir remiamas naujų technologijų, pvz., dirbtinio intelekto, plėtojimas ir integravimas į kibernetinio saugumo didinimo priemones ir programas;

Pakeitimas 115

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies d b punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	db) atvirojo kodo priemonių ir programų integravimo skatinimo politiką;

Pakeitimas 116

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies f punktas

Komisijos siūlomas tekstas	*Pakeitimas*
f) politiką dėl akademinių ir mokslinių tyrimų institucijų rėmimo siekiant tobulinti kibernetinio saugumo priemones ir saugią tinklų infrastruktūrą;	f) politiką dėl akademinių ir mokslinių tyrimų institucijų rėmimo siekiant ***kurti,*** tobulinti ***ir diegti*** kibernetinio saugumo priemones ir saugią tinklų infrastruktūrą;

Pakeitimas 117

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies h punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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.***	h) politiką, kuria ***skatinamas kibernetinis saugumas*** MVĮ, ***įskaitantį*** į šios direktyvos taikymo sritį ***nepatenkančias*** MVĮ, ***tenkinami jų konkretūs*** poreikiai, ir pateikiamos ***lengvai prieinamos*** gairės bei parama***, įskaitant gaires, kaip spręsti tiekimo grandinės problemas;***

Pakeitimas 118

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies h a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ha) politiką, kuria skatinamos kibernetinės higienos programos, apimančios pagrindinį patirties pavyzdžių ir kontrolės priemonių rinkinį, ir didinamas piliečių informuotumas apie kibernetinio saugumo grėsmes ir geriausią patirtį;

Pakeitimas 119

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies h b punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	hb) aktyvios kibernetinės gynybos skatinimo politiką;

Pakeitimas 120

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies h c punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	hc) politiką, kuria valdžios

	institucijoms padedama plėtoti kompetenciją ir suvokimą apie saugumo aspektus, kurie yra būtini projektuojant, kuriant ir valdant susietąsias vietas;

Pakeitimas 121

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies h d punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	hd) politiką, skirtą išpirkos reikalavimo programinės įrangos grėsmei šalinti ir tokios programinės įrangos verslo modeliui išardyti;

Pakeitimas 122

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies h e punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	he) politiką, įskaitant atitinkamas procedūras ir valdymo sistemas, kibernetinio saugumo srities viešojo ir privačiojo sektorių partnerystėms remti ir skatinti.

Pakeitimas 123

Pasiūlymas dėl direktyvos
5 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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 būtina siekiant apsaugoti nacionalinį saugumą.

Pakeitimas 124

Pasiūlymas dėl direktyvos
5 straipsnio 4 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
4. Valstybės narės, remdamosi pagrindiniais veiklos rezultatų rodikliais, vertina savo nacionalines kibernetinio saugumo strategijas ne rečiau kaip kas ketverius metus ir 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.	4. Valstybės narės, remdamosi pagrindiniais veiklos rezultatų rodikliais, vertina savo nacionalines kibernetinio saugumo strategijas ne rečiau kaip kas ketverius metus ir 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. ***ENISA pateikia valstybėms narėms gaires, kad jos suderintų jau parengtas nacionalines kibernetinio saugumo strategijas su šioje direktyvoje nustatytais reikalavimais ir pareigomis.***

Pakeitimas 125

Pasiūlymas dėl direktyvos
6 straipsnio antraštinė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
Suderintas pažeidžiamumų atskleidimas ir Europos pažeidžiamumų ***registras***	Suderintas pažeidžiamumų atskleidimas ir Europos pažeidžiamumų ***duomenų bazė***

Pakeitimas 126

Pasiūlymas dėl direktyvos
6 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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	1. Kiekviena valstybė narė paskiria vieną iš savo CSIRT, kaip nurodyta 9 straipsnyje, koordinuoti suderintą pažeidžiamumų atskleidimą. Paskirta CSIRT veikia kaip patikimas tarpininkas, ***pranešimą teikiančio subjekto prašymu*** lengvinantis sąveiką tarp pranešimą teikiančio subjekto ir gamintojo arba IRT produktų ar IRT paslaugų teikėjo. Jeigu pažeidžiamumas, apie kurį pranešta, yra

gamintojais arba IRT paslaugų teikėjais visoje Sąjungoje, kiekvienos valstybės narės atitinkama paskirtoji CSIRT bendradarbiauja su CSIRT tinklu.	susijęs su įvairiais IRT produktų gamintojais arba IRT paslaugų teikėjais visoje Sąjungoje, kiekvienos valstybės narės atitinkama paskirtoji CSIRT bendradarbiauja su CSIRT tinklu.

Pakeitimas 127

Pasiūlymas dėl direktyvos
6 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	2. ENISA sukuria ir tvarko Europos pažeidžiamumų ***duomenų bazę, kuri papildytų bendri Bendrų pažeidžiamumų ir rizikų (CVE)*** registrą. Tuo tikslu ENISA sukuria ir prižiūri tinkamas informacines sistemas, politiką ir procedūras ***ir priima duomenų bazės saugumui ir vientisumui užtikrinti būtinas techninės ir organizacines priemones***, visų pirma siekdama sudaryti sąlygas svarbiems ir esminiams subjektams bei jų tinklų ir informacinių sistemų tiekėjams***, taip pat ir subjektams, kurie nepatenka į šios direktyvos taikymo sritį, ir jų tiekėjams,*** atskleisti ir registruoti IRT produktų ar paslaugų pažeidžiamumus***.*** Visoms suinteresuotosioms šalims ***suteikiama prieiga*** prie ***duomenų bazėje esančios*** informacijos apie pažeidžiamumus***, kuriems esama pataisų arba poveikio mažinimo priemonių***. ***Duomenų bazėje*** visų pirma pateikiama informacija, kuria apibūdinamas pažeidžiamumas, paveikti IRT produktai ar paslaugos ir pažeidžiamumo rimtumas, atsižvelgiant į aplinkybes, kuriomis jie gali būti naudojami, ***ir*** susijusių pataisų ***buvimas.*** Jei ***pataisų*** nėra, ***į duomenų bazę įtraukiamos*** pažeidžiamų ***IRT*** produktų ir paslaugų naudotojams ***skirtos gairės***, kaip galima sumažinti dėl atskleistų ***pažeidžiamų vietų*** kylančią riziką.

Pakeitimas 128

Pasiūlymas dėl direktyvos
7 straipsnio 1 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	1a. Jeigu valstybė narė paskiria daugiau nei vieną 1 dalyje nurodytą kompetentingą instituciją, ji aiškiai nurodo, kuri iš tų kompetentingų institucijų yra koordinatorė valdant didelio masto incidentus ir krizes.

Pakeitimas 129

Pasiūlymas dėl direktyvos
7 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. Kiekviena valstybė narė, taikydama šią direktyvą, nustato pajėgumus, objektus ir procedūras, kuriais galima pasinaudoti krizės atveju.	2. Kiekviena valstybė narė, taikydama šią direktyvą, nustato pajėgumus, objektus ir procedūras, kuriais galima pasinaudoti krizės atveju.

Pakeitimas 130

Pasiūlymas dėl direktyvos
7 straipsnio 4 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	4. Valstybės narės praneša Komisijai apie savo kompetentingų institucijų paskyrimą, nurodytą 1 dalyje, ir ***Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklui(„EU-CyCLONe“)*** 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.

Pakeitimas 131

Pasiūlymas dėl direktyvos
8 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	3. Kiekviena valstybė narė paskiria vieną ***iš 1 dalyje nurodytų kompetentingų institucijų kaip*** 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.

Pakeitimas 132

Pasiūlymas dėl direktyvos
8 straipsnio 4 dalis

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

Pakeitimas 133

Pasiūlymas dėl direktyvos
9 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. Valstybės narės užtikrina, kad kiekviena CSIRT turėtų tinkamų išteklių, kad galėtų veiksmingai vykdyti savo užduotis, nurodytas 10 straipsnio 2 dalyje.	2. Valstybės narės užtikrina, kad kiekviena CSIRT turėtų tinkamų išteklių ***ir jai būtų sudarytos techninės sąlygos***, kad galėtų veiksmingai vykdyti savo užduotis, nurodytas 10 straipsnio 2 dalyje.

Pakeitimas 134

Pasiūlymas dėl direktyvos
9 straipsnio 6 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	6a. Valstybės narės užtikrina galimybę veiksmingai, efektyviai ir saugiai visais slaptumo žymos laipsniais keistis informacija tarp savo CSIRT ir trečiųjų šalių CSIRT, turinčių patį slaptumo žymos laipsnį.

Pakeitimas 135

Pasiūlymas dėl direktyvos
9 straipsnio 6 b dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	6b. CSIRT, nedarant poveikio Sąjungos teisei, visų pirma Reglamentui (ES) 2016/679, bendradarbiauja su CSIRT arba lygiavertėms įstaigomis šalyse kandidatėse ir kitose trečiosiose šalyse Vakarų Balkanuose ir Rytų partnerystės šalyse ir, kai įmanoma, teikia kibernetinio saugumo pagalbą.

Pakeitimas 136

Pasiūlymas dėl direktyvos
9 straipsnio 7 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	7. Valstybės narės nepagrįstai nedelsdamos praneša Komisijai apie pagal 1 dalį paskirtas CSIRT, CSIRT koordinatorių, paskirtą pagal 6 straipsnio 1 dalį, ***įskaitant*** jų atitinkamas užduotis, kurias jos vykdo ***esminių*** ir ***svarbių*** subjektų atžvilgiu.

Pakeitimas 137

Pasiūlymas dėl direktyvos
10 straipsnio antraštinė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
CSIRT keliami reikalavimai ir užduotys	CSIRT keliami reikalavimai***, techniniai pajėgumai*** ir užduotys

Pakeitimas 138

Pasiūlymas dėl direktyvos
10 straipsnio 1 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
c) CSIRT aprūpinamos tinkama prašymų ***valdymo*** ir ***nukreipimo*** sistema, visų pirma siekiant palengvinti veiksmingą ir efektyvų perdavimą;	c) CSIRT aprūpinamos tinkama prašymų ***klasifikavimo, nukreipimo*** ir ***sekimo*** sistema, visų pirma siekiant palengvinti veiksmingą ir efektyvų perdavimą;

Pakeitimas 139

Pasiūlymas dėl direktyvos
10 straipsnio 1 dalies c a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ca) CSIRT turi tinkamus elgesio kodeksus, kuriais užtikrinamas jų veiklos konfidencialumas ir patikimumas;

Pakeitimas 140

Pasiūlymas dėl direktyvos
10 straipsnio 1 dalies d punktas

Komisijos siūlomas tekstas	*Pakeitimas*
d) CSIRT turi pakankamai darbuotojų, kad būtų užtikrintas pasiekiamumas bet kuriuo metu;	d) CSIRT turi pakankamai darbuotojų, kad būtų užtikrintas pasiekiamumas bet kuriuo metu***, ir užtikrina tinkamas savo darbuotojų mokymo sistemas***;

Pakeitimas 141

Pasiūlymas dėl direktyvos
10 straipsnio 1 dalies e punktas

Komisijos siūlomas tekstas	*Pakeitimas*
e) CSIRT aprūpinamos antrinėmis sistemomis ir atsargine darbo erdve, kad būtų užtikrintas jų paslaugų tęstinumas;	e) CSIRT aprūpinamos antrinėmis sistemomis ir atsargine darbo erdve, kad būtų užtikrintas jų paslaugų tęstinumas***, įskaitant platų tinklų, informacijų sistemų, paslaugų ir įtaisų junglumą***;

Pakeitimas 142

Pasiūlymas dėl direktyvos
10 straipsnio 1 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	1a. CSIRT plėtoja bent šiuos techninius pajėgumus:
	a) gebėjimą tikruoju laiku arba beveik tikruoju laiku stebėti tinklus ir informacines sistemas ir nustatyti anomalijas;
	b) gebėjimą remti įsiskverbimo prevenciją ir nustatymą;
	c) gebėjimą rinkti sudėtingus ekspertizės duomenis ir juos analizuoti, taip pat imtis kibernetinių grėsmių apgrąžos inžinerijos;
	d) gebėjimą filtruoti piktybinį srautą;
	e) gebėjimą užtikrinti griežtą autentiškumo patvirtinimą ir prieigos teises bei kontrolę ir
	f) gebėjimą analizuoti kibernetines grėsmes.

Pakeitimas 143

Pasiūlymas dėl direktyvos
10 straipsnio 2 dalies a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) stebi kibernetines grėsmes, pažeidžiamumus ir incidentus nacionaliniu lygmeniu;	a) stebi kibernetines grėsmes, pažeidžiamumus ir incidentus nacionaliniu lygmeniu ***ir tikruoju laiku gauna žvalgybos informaciją apie grėsmes***;

Pakeitimas 144

Pasiūlymas dėl direktyvos
10 straipsnio 2 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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;	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***, jei įmanoma, tikruoju laiku***;

Pakeitimas 145

Pasiūlymas dėl direktyvos
10 straipsnio 2 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
c) reaguoja į incidentus;	c) reaguoja į incidentus ***ir teikia pagalbą susijusiems subjektams***;

Pakeitimas 146

Pasiūlymas dėl direktyvos
10 straipsnio 2 dalies e punktas

Komisijos siūlomas tekstas	*Pakeitimas*
e) subjekto prašymu aktyviai patikrina tinklų ir informacines sistemas, kurias subjektas naudoja teikdamas paslaugas;	e) subjekto prašymu ***arba kilus rimtai grėsmei nacionaliniam saugumui*** aktyviai patikrina tinklų ir informacines sistemas, kurias subjektas naudoja teikdamas paslaugas;

Pakeitimas 147

Pasiūlymas dėl direktyvos
10 straipsnio 2 dalies f a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	fa) subjekto prašymu teikia tinklo registravimo paslaugas, jas aktyvuoja ir konfigūruoja, siekiant nuo neteisėtos

	eksfiltracijos apsaugoti duomenis, įskaitant asmens duomenis;

Pakeitimas 148

Pasiūlymas dėl direktyvos
10 straipsnio 2 dalies f b punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	fb) prisideda prie saugaus dalijimosi informacija priemonių diegimo pagal 9 straipsnio 3 dalį.

Pakeitimas 149

Pasiūlymas dėl direktyvos
10 straipsnio 4 dalies įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
4. Siekdamos palengvinti bendradarbiavimą, CSIRT skatina priimti ir naudoti bendrą arba standartizuotą praktiką, klasifikavimo sistemas ir taksonomiją srityse, susijusiose su:	4. Siekdamos palengvinti bendradarbiavimą, CSIRT skatina ***automatizuoti keitimąsi informacija,*** priimti ir naudoti bendrą arba standartizuotą praktiką, klasifikavimo sistemas ir taksonomiją srityse, susijusiose su:

Pakeitimas 150

Pasiūlymas dėl direktyvos
11 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.***	2. Valstybės narės užtikrina, kad jų CSIRT gautų pranešimus apie ***reikšmingus*** incidentus ***pagal 20 straipsnį ir*** kibernetines grėsmes ir vos neįvykusius ***incidentus pagal 27 straipsnį per 20 straipsnio 4a dalyje nurodytą vieną langelį.***

Pakeitimas 151

Pasiūlymas dėl direktyvos
11 straipsnio 4 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	4. Tiek, kiek būtina tam, kad šioje direktyvoje nustatytos užduotys ir pareigos būtų vykdomos veiksmingai, valstybės narės užtikrina tinkamą kompetentingų institucijų***,*** bendrųjų informacinių centrų, ***CSIRT,*** teisėsaugos institucijų***, nacionalinių reguliavimo institucijų ar kitų kompetentingų institucijų, atsakingų už viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugas pagal Direktyvą (ES) 2018/1972***, 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 ***pagal jų atitinkamas kompetencijas***.
[39] [įrašyti visą pavadinimą ir OL paskelbimo nuorodą, kai ji bus žinoma]	[39] [įrašyti visą pavadinimą ir OL paskelbimo nuorodą, kai ji bus žinoma]

Pakeitimas 152

Pasiūlymas dėl direktyvos
11 straipsnio 5 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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 saugumo riziką, kibernetines	5. Valstybės narės užtikrina, kad jų kompetentingos institucijos reguliariai ***laiku*** teiktų informaciją pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva] paskirtoms kompetentingoms institucijoms apie kibernetinio 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.	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.

Pakeitimas 153

Pasiūlymas dėl direktyvos
12 straipsnio 3 dalies 1 pastraipa

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

Pakeitimas 154

Pasiūlymas dėl direktyvos
12 straipsnio 3 dalies 2 pastraipa

Komisijos siūlomas tekstas	*Pakeitimas*
Prireikus Bendradarbiavimo grupė gali pakviesti atitinkamų suinteresuotųjų ***šalių*** atstovus dalyvauti jos darbe.	Prireikus Bendradarbiavimo grupė gali pakviesti atitinkamų suinteresuotųjų ***subjektų*** atstovus***, pvz., Europos duomenų apsaugos valdybos ir pramonės atstovus,*** dalyvauti jos darbe.

Pakeitimas 155

Pasiūlymas dėl direktyvos
12 straipsnio 4 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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;	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, standartais ir techninėmis specifikacijomis ***ir esminių ir svarbių subjektų identifikavimu***;

Pakeitimas 156

Pasiūlymas dėl direktyvos
12 straipsnio 4 dalies b a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ba) kartografuoja nacionalinius sprendimus, kad būtų skatinamas kibernetinio saugumo sprendimų, taikomų kiekvienam konkrečiam sektoriui visoje Sąjungoje, suderinamumas;

Pakeitimas 157

Pasiūlymas dėl direktyvos
12 straipsnio 4 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
c) keičiasi patarimais ir bendradarbiauja su Komisija dėl naujų kibernetinio saugumo politikos iniciatyvų;	c) keičiasi patarimais ir bendradarbiauja su Komisija dėl naujų kibernetinio saugumo politikos iniciatyvų ***ir bendro konkretiems sektoriams taikomų kibernetinio saugumo reikalavimų nuoseklumo***;

Pakeitimas 158

Pasiūlymas dėl direktyvos
12 straipsnio 4 dalies f punktas

Komisijos siūlomas tekstas	*Pakeitimas*
f) aptaria 16 straipsnio 7 dalyje nurodytas tarpusavio vertinimo ataskaitas;	f) aptaria 16 straipsnio 7 dalyje nurodytas tarpusavio vertinimo ataskaitas ***ir parengia išvadas ir rekomendacijas***;

Pakeitimas 159

Pasiūlymas dėl direktyvos
12 straipsnio 4 dalies f a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	fa) atlieka suderintus saugumo rizikos vertinimus, kurie gali būti inicijuoti pagal 19 straipsnio 1 dalį, bendradarbiaujant su Komisija ir ENISA;

Pakeitimas 160

Pasiūlymas dėl direktyvos
12 straipsnio 4 dalies k a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ka) 35 straipsnyje nurodytos peržiūros tikslais teikia Komisijai ataskaitas apie strateginiu ir operatyviniu lygmenimis sukauptą patirtį;

Pakeitimas 161

Pasiūlymas dėl direktyvos
12 straipsnio 4 dalies k b punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	kb) bendradarbiaudama su ENISA, Europolu ir nacionalinėmis teisėsaugos institucijomis teikia metinį įvertinimą, kurios trečiosios valstybės priglaudžia išpirkos reikalavimo programinės įrangos nusikaltėlius.

Pakeitimas 162

Pasiūlymas dėl direktyvos
12 straipsnio 8 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	8. Bendradarbiavimo grupė nuolat ir ne rečiau kaip ***du kartus*** per metus susitinka su Ypatingos svarbos subjektų atsparumo klausimų grupe, sudaryta pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva], kad ***palengvintų*** strateginį bendradarbiavimą ir keitimąsi informacija.

Pakeitimas 163

Pasiūlymas dėl direktyvos
13 straipsnio 3 dalies a a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	aa) padeda CSIRT tarpusavyje dalytis technologijomis ir atitinkamomis priemonėmis, politika, geriausia patirtimi ir sistemomis ir jas perduoti;

Pakeitimas 164

Pasiūlymas dėl direktyvos
13 straipsnio 3 dalies b a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ba) užtikrina sąveikumą dalijimosi informacija standartų aspektu;

Pakeitimas 165

Pasiūlymas dėl direktyvos
14 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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,	1. Siekiant remti koordinuotą didelio masto kibernetinio saugumo incidentų ir krizių valdymą veiklos lygmeniu ir užtikrinti reguliarų keitimąsi ***svarbia*** informacija tarp valstybių narių ir Sąjungos

įstaigų ir agentūrų, įsteigiamas Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas („EU-CyCLONe“).	institucijų, įstaigų ir agentūrų, įsteigiamas Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas („EU-CyCLONe“).

Pakeitimas 166

Pasiūlymas dėl direktyvos
14 straipsnio 2 dalis

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

Pakeitimas 167

Pasiūlymas dėl direktyvos
14 straipsnio 5 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
5. „EU-CyCLONe“ reguliariai informuoja Bendradarbiavimo grupę apie ***kibernetines grėsmes,*** incidentus ir tendencijas, ypatingą dėmesį skirdamas jų poveikiui esminiams ir svarbiems subjektams.	5. „EU-CyCLONe“ reguliariai informuoja Bendradarbiavimo grupę apie ***didelio masto*** incidentus ir ***krizes ir apie*** tendencijas, ypatingą dėmesį skirdamas jų poveikiui esminiams ir svarbiems subjektams.

Pakeitimas 168

Pasiūlymas dėl direktyvos
15 straipsnio 1 dalies įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
1. ENISA, bendradarbiaudama su Komisija, kas dvejus metus rengia kibernetinio saugumo Sąjungoje būklės ***ataskaitą***. ***Ataskaitoje*** visų pirma įvertinami šie aspektai:	1. ENISA, bendradarbiaudama su Komisija, kas dvejus metus rengia kibernetinio saugumo Sąjungoje būklės ***ataskaitą ir ją pateikia ir pristato Europos Parlamentui***. ***Ataskaita pateikiama kompiuterio skaitomu formatu ir joje*** visų pirma įvertinami šie aspektai:

Pakeitimas 169

Pasiūlymas dėl direktyvos
15 straipsnio 1 dalies a a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	aa) bendras piliečių ir subjektų, įskaitant MVĮ, informuotumo apie kibernetinį saugumą ir kibernetinės higienos lygį, taip pat bendras susietųjų įrenginių saugumo lygis;

Pakeitimas 170

Pasiūlymas dėl direktyvos
15 straipsnio 1 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
c) kibernetinio saugumo indeksas, kuriame atsispindi apibendrintas kibernetinio saugumo pajėgumų brandos vertinimas.	c) kibernetinio saugumo indeksas, kuriame atsispindi apibendrintas kibernetinio saugumo pajėgumų brandos ***visoje Sąjungoje, įskaitant valstybių narių nacionalinių kibernetinio saugumo strategijų suderinimą,*** vertinimas.

Pakeitimas 171

Pasiūlymas dėl direktyvos
15 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	2. Ataskaitoje ***nustatomos kliūtys ir*** 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.

Pakeitimas 172

Pasiūlymas dėl direktyvos
15 straipsnio 2 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	2a. ENISA, bendradarbiaudama su Komisija bei vadovaujama Bendradarbiavimo grupės ir CSIRT tinklo, parengia metodiką, į kurią būtų įtraukiami atitinkami 1 dalies c punkte nurodyto kibernetinio saugumo indekso kintamieji.

Pakeitimas 173

Pasiūlymas dėl direktyvos
16 straipsnio 1 dalies įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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:	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. ***Tarpusavio vertinimus konsultuodamiesi su ENISA*** atlieka kibernetinio saugumo techniniai ekspertai, atrinkti ***bent*** iš ***dviejų*** valstybių narių, kuriose peržiūra neatlikta, ir jos apima bent šiuos aspektus:

Pakeitimas 174

Pasiūlymas dėl direktyvos
16 straipsnio 1 dalies iii punktas

Komisijos siūlomas tekstas	*Pakeitimas*
iii) CSIRT operatyvinius pajėgumus ir veiksmingumą;	iii) CSIRT operatyvinius pajėgumus ir veiksmingumą ***vykdant savo užduotis***;

Pakeitimas 175

Pasiūlymas dėl direktyvos
16 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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. ***Tarpusavio vertinimą atliekantys paskirti ekspertai prieš pradėdami peržiūrą praneša apie šiuos tikslinius klausimus valstybei narei, kurioje atliekamas vertinimas.***

Pakeitimas 176

Pasiūlymas dėl direktyvos
16 straipsnio 3 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	3a. Prieš pradedant tarpusavio vertinimo procesą, valstybė narė, kurioje atliekamas vertinimas, pati įvertina vertinamus aspektus ir pateikia tą įsivertinimą paskirtiems ekspertams.

Pakeitimas 177

Pasiūlymas dėl direktyvos
16 straipsnio 4 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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	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.

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.	***Komisija, bendradarbiaudama su ENISA, parengia atitinkamus elgesio kodeksus, kuriais grindžiami paskirtų ekspertų darbo metodai.*** 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.

Pakeitimas 178

Pasiūlymas dėl direktyvos
16 straipsnio 6 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
6. Valstybė narė užtikrina, kad bet kokia su paskirtais ekspertais susijusi interesų konflikto rizika būtų ***nepagrįstai nedelsiant*** atskleista kitoms valstybėms narėms, Komisijai ir ENISA.	6. Valstybė narė užtikrina, kad bet kokia su paskirtais ekspertais susijusi interesų konflikto rizika būtų ***prieš pradedant tarpusavio vertinimo procesą*** atskleista kitoms valstybėms narėms, Komisijai ir ENISA.

Pakeitimas 179

Pasiūlymas dėl direktyvos
16 straipsnio 7 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	7. Tarpusavio vertinimuose dalyvaujantys ekspertai parengia per peržiūras nustatytų faktų ir išvadų ataskaitas. ***Ataskaitose pateikiamos rekomendacijos, kaip pagerinti aspektus, kuriuos apėmė tarpusavio vertinimo procesas.*** Ataskaitos teikiamos Komisijai, Bendradarbiavimo grupei, CSIRT tinklui ir ENISA. Ataskaitos aptariamos Bendradarbiavimo grupėje ir CSIRT tinkle. Ataskaitos gali būti skelbiamos Bendradarbiavimo grupės interneto svetainėje***, iš jų pašalinus konfidencialią ir neskelbtiną informaciją***.

Pakeitimas 180

Pasiūlymas dėl direktyvos
17 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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***.	2. Valstybės narės užtikrina, kad ***esminių ir svarbių subjektų*** valdymo organo nariai reguliariai dalyvautų specialiuose mokymuose, ***ir skatina esminius ir svarbius subjektus reguliariai siūlyti panašius mokymus visiems darbuotojams,*** kad ***jie*** įgytų pakankamai žinių ir įgūdžių, kad galėtų suprasti ir įvertinti kibernetinio saugumo riziką ir valdymo praktiką bei jos poveikį subjekto ***teikiamoms paslaugoms***.

Pakeitimas 181

Pasiūlymas dėl direktyvos
18 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	1. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai imtųsi tinkamų ir proporcingų techninių***, operatyvinių*** ir organizacinių priemonių, siekdami valdyti tinklų ir informacinių sistemų, kurias tie subjektai naudoja ***savo veiklai arba*** teikdami savo paslaugas, saugumui kylančią riziką ***ir užkirsti kelią incidentų poveikiui jų paslaugų gavėjams ir kitoms paslaugoms arba juos sumažinti iki minimumo***. Remiantis naujausiais technikos laimėjimais ***ir Europos ir tarptautiniais standartais***, tomis priemonėmis turi būti užtikrinamas toks tinklų ir informacinių sistemų saugumo lygis, kuris atitinka kylančią riziką.

Pakeitimas 182

Pasiūlymas dėl direktyvos
18 straipsnio 2 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
b) incidentų valdymą (incidentų prevencija, aptikimas ir reagavimas į juos);	b) incidentų valdymą;

Pakeitimas 183

Pasiūlymas dėl direktyvos
18 straipsnio 2 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
c) veiklos tęstinumą ir krizių valdymą;	c) veiklos tęstinumą***, pvz., atsarginių kopijų valdymą ir veiklos atkūrimą po ekstremaliųjų įvykių,*** ir krizių valdymą;

Pakeitimas 184

Pasiūlymas dėl direktyvos
18 straipsnio 2 dalies d punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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;	d) tiekimo grandinės saugumą, įskaitant su saugumu susijusius aspektus, susijusius su kiekvieno subjekto ir jo tiekėjų ar paslaugų teikėjų santykiais;

Pakeitimas 185

Pasiūlymas dėl direktyvos
18 straipsnio 2 dalies f punktas

Komisijos siūlomas tekstas	*Pakeitimas*
f) politiką ir procedūras (bandymai ir auditas), skirtas kibernetinio saugumo rizikos valdymo priemonių veiksmingumui įvertinti;	f) politiką ir procedūras (***mokymai,*** bandymai ir auditas), skirtas kibernetinio saugumo rizikos valdymo priemonių veiksmingumui įvertinti;

Pakeitimas 186

Pasiūlymas dėl direktyvos
18 straipsnio 2 dalies f a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	fa) pagrindinę kompiuterių higienos praktiką ir kibernetinio saugumo mokymus;

Pakeitimas 187

Pasiūlymas dėl direktyvos
18 straipsnio 2 dalies g punktas

Komisijos siūlomas tekstas	*Pakeitimas*
g) ***kriptografijos ir*** šifravimo naudojimą.	g) ***atitinkamais atvejais, kriptografijos, pvz.,*** šifravimo***,*** naudojimą.

Pakeitimas 188

Pasiūlymas dėl direktyvos
18 straipsnio 2 dalies g a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ga) kai tinkama, kelių veiksnių tapatumo nustatymo ar nuolatinio tapatumo nustatymo sprendimų, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių ryšių sistemų subjekto viduje naudojimą.

Pakeitimas 189
Pasiūlymas dėl direktyvos
18 straipsnio 4 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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***, tinkamų ir proporcingų*** taisomųjų priemonių, kad atitinkama paslauga atitiktų reikalavimus.

Pakeitimas 190

Pasiūlymas dėl direktyvos
18 straipsnio 5 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	***Išbraukta.***

Pakeitimas 191

Pasiūlymas dėl direktyvos
18 straipsnio 6 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	6. Siekiant atsižvelgti į naujas kibernetines grėsmes, technologinę plėtrą ar sektorių ypatumus, ***taip pat papildyti šią direktyvą, nustatant šio straipsnio 2 dalyje nurodytų priemonių technines ir metodines specifikacijas,*** Komisijai pagal 36 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, kuriais papildomi ***šio straipsnio 2*** dalyje nustatyti aspektai.

Pakeitimas 192

Pasiūlymas dėl direktyvos
19 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	1. Bendradarbiavimo grupė, bendradarbiaudama su Komisija ir ENISA, gali atlikti suderintus konkrečių ypatingos svarbos IRT ***ir ryšių ir informacinės sistemos (RIS)*** paslaugų, sistemų ar produktų tiekimo grandinių saugumo rizikos vertinimus, atsižvelgdama į techninius ir, kai tinkama, netechninius rizikos veiksnius.

Pakeitimas 193

Pasiūlymas dėl direktyvos
19 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	2. Komisija, pasikonsultavusi su Bendradarbiavimo grupe ir ENISA, ***ir, kai tinkama, atitinkamais suinteresuotaisiais subjektais,*** nustato konkrečias ypatingos svarbos IRT ***ir RIS*** paslaugas, sistemas ar produktus, dėl kurių gali būti atliekamas 1 dalyje nurodytas koordinuotas rizikos vertinimas.

Pakeitimas 194

Pasiūlymas dėl direktyvos
20 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	1. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai nepagrįstai nedelsdami praneštų CSIRT pagal 3 ir 4 dalis apie bet kokį ***reikšmingą incidentą***. Valstybės narės užtikrina, kad tie subjektai, be kita ko, praneštų visą informaciją, pagal kurią kompetentingos institucijos arba CSIRT galėtų nustatyti tarpvalstybinį incidento poveikį.

Pakeitimas 195

Pasiūlymas dėl direktyvos
20 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	Kai ***tinkama, valstybės narės užtikrina***, ***kad esminiai ir svarbūs*** subjektai nepagrįstai nedelsdami ***informuotų*** savo paslaugų ***gavėjus apie apsaugos nuo tam tikrų incidentų ir žinomos rizikos*** priemones ar ***taisomąsias*** priemones, kurių ***gali imtis*** gavėjai***. Kai tinkama, subjektai informuoja savo paslaugų gavėjus apie patį incidentą arba žinomą riziką. Gavėjai informuojami dedant visas pastangas, o*** dėl ***šio informavimo*** pranešančiojo subjekto atsakomybė nepadidėja.

Pakeitimas 196

Pasiūlymas dėl direktyvos
20 straipsnio 3 dalies įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
3. ***Incidentas laikomas rimtu***, ***jeigu***:	3. ***Siekiant nustatyti incidento svarbą, kai įmanoma***, ***atsižvelgiama į šiuos parametrus***:

Pakeitimas 197

Pasiūlymas dėl direktyvos
20 straipsnio 3 dalies a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) ***dėl incidento atitinkamas subjektas patyrė arba gali patirti didelių veiklos sutrikimų arba finansinių nuostolių***;	a) ***paslaugų, kurias paveikė incidentas, gavėjų skaičių***;

Pakeitimas 198

Pasiūlymas dėl direktyvos
20 straipsnio 3 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
b) ***incidentas paveikė arba gali paveikti kitus fizinius ar juridinius asmenis dėl didelių materialinių arba neturtinių nuostolių.***	b) ***incidento trukmę;***

Pakeitimas 199

Pasiūlymas dėl direktyvos
20 straipsnio 3 dalies b a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ba) geografinę teritoriją, kurioje incidentas daro poveikį;

Pakeitimas 200

Pasiūlymas dėl direktyvos
20 straipsnio 3 dalies b b punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	bb) incidento poveikio paslaugos veikimui ir tęstinumui mastą;

Pakeitimas 201

Pasiūlymas dėl direktyvos
20 straipsnio 3 dalies b c punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	bc) incidento poveikio ekonominei ir visuomeninei veiklai mastą.

Pakeitimas 202

Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies 1 pastraipos įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
Valstybės narės užtikrina, kad 1 dalyje nurodyto pranešimo tikslais atitinkami subjektai ***kompetentingoms institucijoms***	Valstybės narės užtikrina, kad 1 dalyje nurodyto pranešimo tikslais atitinkami subjektai CSIRT pateiktų:

arba CSIRT pateiktų:

Pakeitimas 203

Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies 1 pastraipos a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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;***	a) ***pradinį pranešimą apie reikšmingą*** incidentą, ***kuriame pateikiama informacija***, ***kurią dėdamas visas pastangas gali gauti pranešantysis subjektas***, ***tokia tvarka:***

Pakeitimas 204

Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies 1 pastraipos a punkto i papunktis (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	i) įvykus incidentui, kuris rimtai sutrikdo subjekto teikiamų paslaugų prieinamumą, CSIRT apie jį turi būti pranešama nedelsiant ir bet kuriuo atveju ne vėliau kaip per 24 valandas nuo tos tada, kai sužinoma apie incidentą;

Pakeitimas 205

Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies 1 pastraipos a punkto ii papunktis (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ii) įvykus incidentui, kuris daro kitokį reikšmingą poveikį subjektui, tačiau ne to subjekto teikiamų paslaugų prieinamumui, CSIRT apie jį turi būti pranešama nepagrįstai nedelsiant ir bet kuriuo atveju ne vėliau kaip per 72 valandas nuo tos tada, kai sužinoma apie incidentą;

Pakeitimas 206

Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies 1 pastraipos a punkto iii papunktis (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	iii) įvykus incidentui, kuris daro reikšmingą poveikį patikimumo užtikrinimo paslaugų teikėjo, apibrėžto Reglamento (ES) Nr. 910/2014 3 straipsnio 19 punkte, paslaugoms arba to patikimumo užtikrinimo paslaugų teikėjo saugomiems asmens duomenims, CSIRT apie jį turi būti pranešama nedelsiant ir bet kuriuo atveju ne vėliau kaip per 24 valandas nuo tos tada, kai sužinoma apie incidentą;

Pakeitimas 207

Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies 1 pastraipos b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
b) ***kompetentingos institucijos arba*** CSIRT prašymu – tarpinę ataskaitą apie atitinkamus atnaujintus duomenis apie padėtį;	b) CSIRT prašymu – tarpinę ataskaitą apie atitinkamus atnaujintus duomenis apie padėtį;

Pakeitimas 208

Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies 1 pastraipos c punkto įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
c) ne vėliau kaip per vieną mėnesį nuo ***a punkte nurodytos ataskaitos*** pateikimo – ***galutinę*** ataskaitą, kurioje pateikiama bent ši informacija:	c) ne vėliau kaip per vieną mėnesį nuo ***pradinio pranešimo*** pateikimo – ***išsamią*** ataskaitą, kurioje pateikiama bent ši informacija:

Pakeitimas 209

Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies 1 pastraipos c a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ca) jei teikiant išsamią ataskaitą pagal c punktą incidentas tebevyksta, galutinė ataskaita pateikiama praėjus mėnesiui po to, kai incidentas išsprendžiamas.

Pakeitimas 210

Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies 2 pastraipa

Komisijos siūlomas tekstas	*Pakeitimas*
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.	Valstybės narės nustato, kad tinkamai pagrįstais atvejais ir susitarus su CSIRT atitinkamas subjektas gali nukrypti nuo a ***punkto i*** ir ***ii papunkčiuose bei*** c ***punkte*** nustatytų terminų. ***Valstybės narės užtikrina neskelbtinos informacijos apie incidentus, kuria dalijamasi su CSIRT, konfidencialumą ir tinkamą apsaugą ir priima dalijimosi informacija apie incidentus ir jos pakartotinio naudojimo priemones ir procedūras.***

Pakeitimas 211

Pasiūlymas dėl direktyvos
20 straipsnio 4 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	4a. Valstybės narės nustato vieną langelį pateikti visiems pranešimams, kurių reikalaujama pagal šią direktyvą ir kitus susijusius Sąjungos teisės aktus. ENISA, bendradarbiaudama su Bendradarbiavimo grupe, parengia ir nuolat tobulina bendrus pranešimo šablonus, pateikdama gaires, kuriomis supaprastinama ir racionalizuojama pagal Sąjungos teisę reikalaujama pranešimų teikimo informacija ir sumažinama pranešantiesiems subjektams tenkanti našta.

Pakeitimas 212

Pasiūlymas dėl direktyvos
20 straipsnio 4 b dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	4b. Esminiai ir svarbūs subjektai, nurodyti 24 straipsnio 1 dalyje, gali atitikti šio straipsnio 1 dalies reikalavimus pateikdami pranešimą valstybės narės, kurioje subjektai turi pagrindinę buveinę Sąjungoje, CSIRT ir pranešdami esminiams ir svarbiems subjektams, kuriems jie teikia paslaugas, dėl bet kokio reikšmingo incidento, kuris yra žinomas kaip darantis poveikį paslaugų gavėjui.

Pakeitimas 213

Pasiūlymas dėl direktyvos
20 straipsnio 5 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	5. 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 ***ir įgyvendinamų patarimų***. CSIRT teikia papildomą techninę pagalbą, jei to prašo atitinkamas subjektas. Jei įtariama, kad incidentas yra baudžiamojo pobūdžio, CSIRT taip pat teikia gaires dėl pranešimo apie incidentą teisėsaugos institucijoms. ***CSIRT gali dalytis informacija apie incidentą su kitais svarbiais ir esminiais subjektais, kartu užtikrindama pranešančiojo subjekto pateiktos informacijos konfidencialumą.***

Pakeitimas 214

Pasiūlymas dėl direktyvos
20 straipsnio 6 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	6. Atitinkamais atvejais ir visų pirma tuomet, kai 1 dalyje nurodytas incidentas susijęs su dviem ar daugiau valstybių narių, CSIRT apie incidentą informuoja kitas paveiktas valstybes nares ir ENISA ***ir pateikia joms svarbią informaciją***. Tai ***darydami*** 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.

Pakeitimas 215

Pasiūlymas dėl direktyvos
20 straipsnio 7 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	7. Kai visuomenės informuotumas yra būtinas siekiant užkirsti kelią incidentui ar reaguoti į besitęsiantį incidentą arba kai incidento atskleidimas kitais atvejais atitinka viešąjį interesą, CSIRT ir atitinkamais atvejais kitų atitinkamų valstybių narių CSIRT, pasikonsultavusios su atitinkamu subjektu, gali informuoti visuomenę apie incidentą arba pareikalauti, kad tai padarytų subjektas.

Pakeitimas 216

Pasiūlymas dėl direktyvos
20 straipsnio 7 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	7a. CSIRT bendrajam informaciniam centrui ir, kai tinkama, kompetentingoms

	institucijoms nepagrįstai nedelsdamos teikia informaciją apie reikšmingus incidentus, apie kuriuos buvo pranešta pagal 1 dalį.

Pakeitimas 217

Pasiūlymas dėl direktyvos
20 straipsnio 8 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
8. ***Kompetentingos institucijos arba CSIRT*** prašymu bendrasis informacinis centras perduoda pagal 1 ***ir 2 dalis*** gautus pranešimus kitų paveiktų valstybių narių bendriesiems informaciniams centrams.	8. ***CSIRT*** prašymu bendrasis informacinis centras perduoda pagal 1 ***dalį*** gautus pranešimus kitų paveiktų valstybių narių bendriesiems informaciniams centrams***, užtikrindamas pranešančiojo subjekto pateiktos informacijos konfidencialumą ir tinkamą apsaugą***.

Pakeitimas 218

Pasiūlymas dėl direktyvos
20 straipsnio 9 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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 ***šio straipsnio 1 dalį*** ir 27 straipsnį. Siekdama prisidėti prie palyginamos informacijos teikimo ENISA gali paskelbti technines gaires dėl į suvestinę ataskaitą įtrauktos informacijos parametrų.

Pakeitimas 219

Pasiūlymas dėl direktyvos
20 straipsnio 10 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
10. Kompetentingos institucijos pagal Direktyvą (ES) XXXX/XXXX [Ypatingos	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].	svarbos subjektų atsparumo direktyva] paskirtoms kompetentingoms institucijoms teikia informaciją apie incidentus ir kibernetines grėsmes, apie kuriuos pagal ***šio straipsnio*** 1 ***dalį*** ir ***27 straipsnį*** pranešė esminiai subjektai, nustatyti kaip ypatingos svarbos subjektai arba ypatingos svarbos subjektams lygiaverčiai subjektai, pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva].

Pakeitimas 220

Pasiūlymas dėl direktyvos
20 straipsnio 11 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	11. Komisija gali priimti įgyvendinimo aktus, kuriais išsamiau nustatoma pagal ***šio straipsnio*** 1 ***dalį*** ir ***27 straipsnį*** pateikto pranešimo rūšis, formatas ir procedūra. Tie įgyvendinimo aktai priimami laikantis 37 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

Pakeitimas 221

Pasiūlymas dėl direktyvos
20 straipsnio 11 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	11a. Komisijai pagal 36 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, kuriais ši direktyva papildoma nustatant informacijos, kuri turi būti pateikta pagal šio straipsnio 1 dalį, tipą ir patikslinant parametrus, į kuriuos turi būti atsižvelgiama nustatant incidento poveikio mastą, kaip nurodyta šio straipsnio 3 dalyje.

Pakeitimas 222

Pasiūlymas dėl direktyvos
21 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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***.	1. ***Valstybės narės, vadovaudamosi ENISA***, ***Komisijos ir bendradarbiavimo grupės rekomendacijomis***, ***skatina esminius*** ir ***svarbius subjektus sertifikuoti*** tam tikrus IRT produktus, paslaugas ir procesus***, kuriuos kuria esminis arba svarbus subjektas arba kurie perkami iš trečiųjų šalių, pagal*** Europos kibernetinio saugumo schemas, priimtas pagal Reglamento (ES) 2019/881 49 ***straipsnį, arba, jei tokių schemų dar nėra, pagal panašias tarptautiniu mastu pripažintas sertifikavimo schemas***. ***Be to***, ***valstybės narės skatina esminius ir svarbius subjektus naudotis kvalifikuotomis patikimumo užtikrinimo paslaugomis pagal Reglamentą (ES) Nr. 910/2014***.

Pakeitimas 223

Pasiūlymas dėl direktyvos
21 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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***.	2. Komisijai ***pagal 36 straipsnį*** suteikiami įgaliojimai priimti deleguotuosius aktus, kuriais ***ši direktyva papildoma nustatant***, kokių kategorijų esminiams ***ir svarbiems*** subjektams reikia gauti sertifikatą ir pagal kurias konkrečias Europos kibernetinio saugumo sertifikavimo schemas pagal ***Reglamento (ES) 2019/881 49 straipsnį***. ***Priimti tokius deleguotuosius aktus galima svarstyti tais atvejais, kai nustatomi nepakankami kibernetinio saugumo lygiai, prieš juos priimant turi būti atliekamas poveikio vertinimas ir juose numatomas įgyvendinimo laikotarpis***.

Pakeitimas 224

Pasiūlymas dėl direktyvos
21 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	3. Komisija***, pasikonsultavusi su bendradarbiavimo grupe ir Europos kibernetinio saugumo sertifikavimo grupe,*** gali prašyti ENISA parengti potencialią schemą pagal Reglamento (ES) 2019/881 48 straipsnio 2 dalį tais atvejais, kai nėra tinkamos Europos kibernetinio saugumo sertifikavimo schemos 2 dalies tikslais.

Pakeitimas 225

Pasiūlymas dėl direktyvos
22 straipsnio 2 dalis

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

Pakeitimas 226

Pasiūlymas dėl direktyvos
22 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
	3. Komisija, bendradarbiaudama su ENISA, remia ir skatina standartų, kuriuos nustatė atitinkamos Sąjungos ir tarptautinės standartizacijos institucijos siekdamos vienodai įgyvendinti 18 straipsnio 1 ir 2 dalis, rengimą ir įgyvendinimą. Komisija remia standartų

atnaujinimą atsižvelgiant į technologijų plėtrą.

Pakeitimas 227

Pasiūlymas dėl direktyvos
23 straipsnio antraštinė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
Domenų vardų ir registracijos duomenų ***bazės***	Domenų vardų ir registracijos duomenų ***bazių struktūra***

Pakeitimas 228

Pasiūlymas dėl direktyvos
23 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.***	1. Siekdamos prisidėti prie DNS saugumo, stabilumo ir atsparumo, valstybės narės ***reikalauja***, kad aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys domenų vardų registravimo paslaugas, ***rinktų ir šiais tikslais naudojamoje*** duomenų ***bazių struktūroje*** saugotų tikslius***, patikrintus*** ir išsamius domenų vardų registracijos duomenis***.***

Pakeitimas 229

Pasiūlymas dėl direktyvos
23 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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	2. Valstybės narės užtikrina, kad 1 dalyje ***nurodytoje*** domenų vardų registracijos duomenų ***bazių struktūroje*** būtų atitinkama informacija***, įskaitant bent jau registruotojų pavadinimus, jų faktinius ir e. pašto adresus bei telefono numerius***, pagal kurią būtų galima

pažymėtus domenų vardus, ir su jais susisiekti.	nustatyti domenų vardų turėtojus ir kontaktinius centrus, administruojančius aukščiausio lygio domenų vardais pažymėtus domenų vardus, ir su jais susisiekti.

Pakeitimas 230

Pasiūlymas dėl direktyvos
23 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	3. Valstybės narės užtikrina, kad aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys domenų vardų registravimo paslaugas, taikytų politiką ir procedūras, kuriomis užtikrinama, kad duomenų ***bazių struktūroje*** būtų pateikiama tiksli***, patikinta*** ir išsami informacija. Valstybės narės užtikrina, kad tokia politika ir procedūros būtų skelbiamos viešai.

Pakeitimas 231

Pasiūlymas dėl direktyvos
23 straipsnio 4 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	4. Valstybės narės užtikrina, kad aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys domenų vardų registravimo paslaugas, nepagrįstai nedelsdami po domeno vardo užregistravimo ***viešai*** paskelbtų domeno registracijos duomenis, kurie nėra asmens duomenys. ***Tais atvejais, kai registruotojai yra juridiniai asmenys, viešai skelbiami domeno registracijos duomenys apima bent registruotojo pavadinimą, jo fizinį ir e. pašto adresą ir telefono numerį.***

Pakeitimas 232

Pasiūlymas dėl direktyvos
23 straipsnio 5 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	5. Valstybės narės ***reikalauja***, kad aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys domenų vardų registravimo paslaugas, gavę tinkamai pagrįstus siekiančių gauti prieigą subjektų prašymus, suteiktų prieigą prie konkrečių domenų vardų registracijos duomenų, ***įskaitant asmens duomenis,*** laikydamiesi Sąjungos duomenų apsaugos teisės aktų. Valstybės narės ***reikalauja***, kad aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys domenų vardų registravimo paslaugas***, atsakytų į visus prašymus suteikti prieigą*** nepagrįstai nedelsdami ***ir bet kuriuo atveju per 72 valandas nuo tada, kai gaunamas prašymas*** suteikti prieigą. Valstybės narės užtikrina, kad tokių duomenų atskleidimo politika ir procedūros būtų skelbiamos viešai.

Pakeitimas 233

Pasiūlymas dėl direktyvos
24 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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 ***arba*** valstybėje narėje, kurioje subjekto padalinyje dirba daugiausia darbuotojų Sąjungoje***, arba valstybėje narėje, kurioje vykdomos kibernetinio saugumo operacijos***.

Pakeitimas 234

Pasiūlymas dėl direktyvos
25 straipsnio antraštinė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
Esminių ir svarbių subjektų registras	***ENISA*** registras

Pakeitimas 235

Pasiūlymas dėl direktyvos
25 straipsnio 1 dalies įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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:	1. ENISA sukuria ir tvarko 24 straipsnio 1 dalyje ***saugų*** nurodytų esminių ir svarbių subjektų registrą***, į jį įtraukdama*** šią informaciją:

Pakeitimas 236

Pasiūlymas dėl direktyvos
25 straipsnio 1 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
c) ***naujausius*** kontaktinius duomenis, įskaitant ***subjektų*** e. pašto adresus ***ir*** telefono numerius.	c) ***aktualius*** kontaktinius duomenis, įskaitant e. pašto adresus***, IP adresus,*** telefono numerius ***ir atitinkamus subjektų sektorius ir pasektorius, nurodytus I ir II prieduose***.

Pakeitimas 237

Pasiūlymas dėl direktyvos
25 straipsnio 1 dalies 1 a pastraipa (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	Ne vėliau kaip ... [12 mėnesių po šios direktyvos įsigaliojimo dienos] esminiai ir svarbūs subjektai pirmoje pastraipoje nurodytą informaciją pateikia ENISA.

Pakeitimas 238

Pasiūlymas dėl direktyvos
26 straipsnio 1 dalies įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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:	1. ***Valstybės*** narės užtikrina, kad esminiai ir svarbūs subjektai ***bei kiti susiję subjektai, kuriems netaikoma šios direktyvos taikymo sritis,*** galėtų tarpusavyje keistis svarbia kibernetinio saugumo informacija, įskaitant informaciją, susijusią su kibernetinėmis grėsmėmis***, vos neįvykusiais incidentais***, pažeidžiamumu, ***metodais ir procedūromis, metaduomenimis ir turinio duomenimis,*** užvaldymo rodikliais, ***priešiška*** taktika, **modus operandi*, konkrečių dalyvių informacija***, kibernetinio saugumo perspėjimais***, pramoninio šnipinėjimo taktika,*** ir ***rekomenduojamomis apsaugos priemonės konfigūracijomis***, kai tokiu dalijimusi informacija:

Pakeitimas 239

Pasiūlymas dėl direktyvos
26 straipsnio 1 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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***, sustabdymo ir prevencijos*** metodus, švelninimo strategijas ***ar*** reagavimo ir atsigavimo etapus***, arba skatinant bendrai viešųjų ir privačiųjų subjektų atliekamus bendradarbiavimu grindžiamus kibernetinių grėsmių mokslinius tyrimus***.

Pakeitimas 240

Pasiūlymas dėl direktyvos
26 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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***.	2. Valstybės narės ***sudaro palankesnes sąlygas keistis*** informacija ***sudarydamos sąlygas steigti patikimas*** esminių ir svarbių subjektų ***ir jų paslaugų teikėjų bei, kai tinkama, kitų tiekėjų bendruomenes***. Toks keitimasis vykdomas taikant dalijimosi informacija susitarimus, susijusius su galimai neskelbtina informacija, kuria keičiamasi.

Pakeitimas 241

Pasiūlymas dėl direktyvos
26 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	3. Valstybės narės ***sudaro palankias sąlygas sudaryti*** 2 dalyje ***nurodytus*** dalijimosi ***kibernetinio saugumo*** informacija ***susitarimus, suteikdamos*** veiklos ***elementus*** (įskaitant specialių IRT platformų ***ir r automatizavimo*** naudojimą) ***bei turinį***. ***Valstybės narės nustato išsamią informaciją*** apie valdžios institucijų dalyvavimą tokiuose susitarimuose, ***ir gali nustatyti tam tikras sąlygas dėl informacijos***, ***kurią pateikia kompetentingos institucijos arba CSIRT***. Valstybės narės teikia paramą tokių priemonių taikymui pagal 5 straipsnio 2 dalies g punkte nurodytą savo politiką.

Pakeitimas 242

Pasiūlymas dėl direktyvos
27 straipsnio 1 pastraipa

Komisijos siūlomas tekstas	*Pakeitimas*
Valstybės narės užtikrina, kad***, nedarant poveikio 3 straipsniui, subjektai, kuriems ši direktyva netaikoma, galėtų*** savanoriškai ***teikti*** pranešimus ***apie didelius incidentus, kibernetines grėsmes***	Valstybės narės užtikrina, kad savanoriškai pranešimus ***CIRT galėtų*** teikti***:***

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.

Pakeitimas 243

Pasiūlymas dėl direktyvos
27 straipsnio 1 pastraipos a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	a) esminiai ir svarbūs subjektai (pranešimus apie kibernetines grėsmes ir vos neįvykusius incidentus);

Pakeitimas 244

Pasiūlymas dėl direktyvos
27 straipsnio 1 pastraipos b punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	b) subjektai, nepatenkantys į šios direktyvos taikymo sritį (pranešimus apie reikšmingus incidentus, kibernetines grėsmes ir vos neįvykusius incidentus).

Pakeitimas 245

Pasiūlymas dėl direktyvos
27 straipsnio 1 pastraipos 1 a pastraipa (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	Tvarkydamos tokius pranešimus valstybės narės veikia pagal 20 straipsnyje nustatytą procedūrą. Valstybės narės gali teikti pirmenybę privalomų pranešimų tvarkymui, lyginant su savanoriškais pranešimais. Prireikus CSIRT teikia

	bendrajam informaciniam centrui ir, kai tinkama, kompetentingoms institucijoms informaciją apie pagal šį straipsnį gautus pranešimus, kartu užtikrindamos pranešančiojo subjekto pateiktos informacijos konfidencialumą ir tinkamą apsaugą. Dėl savanoriško pranešimo pranešančiajam subjektui nenustatoma jokių papildomų pareigų, kurios jam nebūtų taikomos, jei jis nebūtų pateikęs pranešimo.

Pakeitimas 246

Pasiūlymas dėl direktyvos
28 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. Kompetentingos institucijos, nagrinėdamos incidentus, dėl kurių pažeidžiamas asmens duomenų saugumas, glaudžiai bendradarbiauja su duomenų apsaugos institucijomis.	2. Kompetentingos institucijos, nagrinėdamos incidentus, dėl kurių pažeidžiamas asmens duomenų saugumas, glaudžiai bendradarbiauja su duomenų apsaugos institucijomis. ***Tai turi būti daroma atsižvelgiant į jų kompetenciją ir užduotis pagal Reglamentą (ES) 2016/679.***

Pakeitimas 247

Pasiūlymas dėl direktyvos
29 straipsnio 2 dalies a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) atlikti patikrinimus vietoje ir priežiūrą ne vietoje, įskaitant atsitiktinius patikrinimus;	a) atlikti patikrinimus vietoje ir priežiūrą ne vietoje, įskaitant atsitiktinius patikrinimus***, kuriuos atlieka apmokyti specialistai***;

Pakeitimas 248

Pasiūlymas dėl direktyvos
29 straipsnio 2 dalies a a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	aa) atlikti reikalavimų nesilaikymo

	atvejų ir jų poveikio paslaugų saugumui tyrimus;

Pakeitimas 249

Pasiūlymas dėl direktyvos
29 straipsnio 2 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
b) atlikti ***reguliarius*** auditus;	b) atlikti ***metinius ir tikslinius saugumo*** auditus***, kuriuos vykdo kvalifikuota nepriklausoma įstaiga arba kompetentinga institucija***;

Pakeitimas 250

Pasiūlymas dėl direktyvos
29 straipsnio 2 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
c) atlikti ***tikslingus saugumo*** auditus, ***pagrįstus rizikos vertinimais arba prieinama informacija apie riziką***;	c) atlikti **ad hoc** auditus ***tais atvejais***, ***kai tai pateisinama dėl svarbaus incidento arba esminio subjekto neatitikties***;

Pakeitimas 251

Pasiūlymas dėl direktyvos
29 straipsnio 2 dalies 1 a ir 1 b pastraipos (naujos)

Komisijos siūlomas tekstas	*Pakeitimas*
	Pirmos pastraipos b punkte nurodyti tiksliniai saugumo auditai grindžiami kompetentingos institucijos arba audituojamo subjekto atliktais rizikos vertinimais arba kita turima su rizika susijusia informacija.
	Bet kokio tikslinio saugumo audito rezultatai pateikiami kompetentingai institucijai. Tokio tikslinio saugumo audito, kurį atlieka kvalifikuota nepriklausoma įstaiga, išlaidas apmoka atitinkamas subjektas.

Pakeitimas 252

Pasiūlymas dėl direktyvos
29 straipsnio 2 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	2a. Naudodamosi savo įgaliojimais pagal 2 dalies a–d punktus kompetentingos institucijos kuo labiau sumažina poveikį subjekto poveikį verslo procesams;

Pakeitimas 253

Pasiūlymas dėl direktyvos
29 straipsnio 4 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
b) priimti privalomus nurodymus arba įsakymą, kuriuo reikalaujama, kad tie subjektai pašalintų nustatytus trūkumus arba šioje direktyvoje nustatytų pareigų pažeidimus;	b) priimti privalomus nurodymus***, įskaitant nurodymus dėl priemonių, kurių reikia užkirsti kelią incidentui arba jam išspręsti, ir tokių priemonių įgyvendinimo bei ataskaitų apie jų įgyvendinimą terminus,*** arba įsakymą, kuriuo reikalaujama, kad tie subjektai pašalintų nustatytus trūkumus arba šioje direktyvoje nustatytų pareigų pažeidimus;

Pakeitimas 254

Pasiūlymas dėl direktyvos
29 straipsnio 4 dalies i punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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;	***Išbraukta.***

Pakeitimas 255

Pasiūlymas dėl direktyvos
29 straipsnio 4 dalies j punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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.	j) skirti arba prašyti, kad atitinkamos įstaigos ar teismai pagal ***nacionalinę teisę*** skirtų administracinę baudą pagal 31 straipsnį, kartu su šios dalies a–i punktuose nurodytomis priemonėmis, atsižvelgiant į kiekvieno atskiro atvejo aplinkybes.

Pakeitimas 256

Pasiūlymas dėl direktyvos
29 straipsnio 5 dalies 1 pastraipos a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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;	a) ***laikinai*** sustabdyti arba prašyti, kad sertifikavimo arba leidimus išduodanti įstaiga ***laikinai*** sustabdytų sertifikavimą arba įgaliojimą, susijusį su dalimi arba visomis esminės įstaigos teikiamomis ***atitinkamomis*** paslaugomis ar veikla;

Pakeitimas 257

Pasiūlymas dėl direktyvos
29 straipsnio 5 dalies 1 pastraipos b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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.	b) ***kaip* ultima ratio** reikalauti, kad atitinkamos įstaigos ar teismai pagal ***nacionalinę teisę*** nustatytų laikiną draudimą bet kuriam tame pagrindiniame subjekte vadovaujamas pareigas einančiam asmeniui arba teisiniam atstovui tame subjekte eiti vadovaujamas pareigas tame subjekte.

Pakeitimas 258

Pasiūlymas dėl direktyvos
29 straipsnio 5 dalies 2 pastraipa

Komisijos siūlomas tekstas	*Pakeitimas*
Šios sankcijos taikomos tik tol, kol subjektas ***imasi*** būtinų veiksmų trūkumams pašalinti arba kompetentingos institucijos, kuriai taikytos tokios sankcijos, reikalavimams įvykdyti.	***Laikini sustabdymai arba draudimai pagal šią dalį taikomi*** tik tol, kol ***atitinkamas*** subjektas ***nesiims*** būtinų veiksmų trūkumams pašalinti arba kompetentingos institucijos, kuriai taikytos tokios sankcijos, reikalavimams įvykdyti. ***Skiriant tokius laikinus sustabdymus ar draudimus, turėtų būti taikomos tinkamos procedūrinės apsaugos priemonės pagal bendruosius Sąjungos teisės ir Chartijos principus, įskaitant veiksmingą teisminę apsaugą, tinkamą procesą, nekaltumo prezumpciją ir teisę į gynybą;***

Pakeitimas 259

Pasiūlymas dėl direktyvos
29 straipsnio 7 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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;	c) padarytą žalą ar patirtus nuostolius, ***įskaitant*** faktinius ar galimus finansinius ar ekonominius nuostolius, poveikį kitoms paslaugoms ***ir*** paveiktų naudotojų skaičių;

Pakeitimas 260

Pasiūlymas dėl direktyvos
29 straipsnio 7 dalies c a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ca) bet kuriuos to atitinkamo subjekto svarbius ankstesnius pažeidimus;

Pakeitimas 261

Pasiūlymas dėl direktyvos
29 straipsnio 9 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	9. Valstybės narės užtikrina, kad jų kompetentingos institucijos informuotų atitinkamas ***visų susijusių valstybių narių*** 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.

Pakeitimas 262

Pasiūlymas dėl direktyvos
29 straipsnio 9 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	9a. Valstybės narės užtikrina, kad jų kompetentingos institucijos bendradarbiautų su atitinkamomis atitinkamos valstybės narės kompetentingomis institucijomis, paskirtomis pagal Reglamentą (ES) XXXX/XXXX [DORA].

Pakeitimas 263

Pasiūlymas dėl direktyvos
30 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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. ***Valstybės narės užtikrina, kad tos priemonės būtų veiksmingos, proporcingos ir atgrasančios, atsižvelgiant į kiekvieno atskiro atvejo aplinkybes.***

Pakeitimas 264

Pasiūlymas dėl direktyvos
30 straipsnio 2 dalies a punktas

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

Pakeitimas 265

Pasiūlymas dėl direktyvos
30 straipsnio 2 dalies a a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	aa) atlikti reikalavimų nesilaikymo atvejų ir jų poveikio paslaugų saugumui tyrimus;

Pakeitimas 266

Pasiūlymas dėl direktyvos
30 straipsnio 2 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
b) atlikti ***tikslingus*** saugumo auditus, ***pagrįstus rizikos vertinimais arba prieinama informacija apie riziką***;	b) atlikti ***tikslinius*** saugumo auditus, ***kuriuos vykdo kvalifikuota nepriklausoma įstaiga arba kompetentinga institucija***;

Pakeitimas 267

Pasiūlymas dėl direktyvos
30 straipsnio 2 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
c) atlikti saugumo patikrinimus, pagrįstus objektyviais, sąžiningais ir skaidriais rizikos vertinimo kriterijais;	c) atlikti saugumo patikrinimus, pagrįstus objektyviais, nediskriminaciniais, sąžiningais ir skaidriais rizikos vertinimo kriterijais;

Pakeitimas 268

Pasiūlymas dėl direktyvos
30 straipsnio 2 dalies 1 a ir 1 b pastraipos (naujos)

Komisijos siūlomas tekstas	*Pakeitimas*
	Pirmos pastraipos b punkte nurodyti tiksliniai saugumo auditai grindžiami kompetentingos institucijos arba audituojamo subjekto atliktais rizikos vertinimais arba kita turima su rizika susijusia informacija.
	Bet kokio tikslinio saugumo audito rezultatai pateikiami kompetentingai institucijai. Tokio tikslinio saugumo audito, kurį atlieka kvalifikuota nepriklausoma įstaiga, išlaidas apmoka atitinkamas subjektas.

Pakeitimas 269

Pasiūlymas dėl direktyvos
30 straipsnio 4 dalies h punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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;	***Išbraukta.***

Pakeitimas 270

Pasiūlymas dėl direktyvos
30 straipsnio 4 dalies i punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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.	i) skirti arba prašyti, kad atitinkamos įstaigos ar teismai pagal ***nacionalinę teisę*** skirtų administracinę baudą pagal 31 straipsnį, kartu su šios dalies ***a–h*** punktuose nurodytomis priemonėmis, atsižvelgiant į kiekvieno atskiro atvejo aplinkybes.

Pakeitimas 271

Pasiūlymas dėl direktyvos
31 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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***.	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.

Pakeitimas 272

Pasiūlymas dėl direktyvos
32 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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 informuoja priežiūros institucijas, kompetentingas pagal to reglamento 55 ir 56 straipsnius***, nepagrįstai nedelsdamos ir bet kuriuo atveju per 72 valandas nuo tada, kai***

sužino apie pažeistą duomenų saugumą.

Pakeitimas 273

Pasiūlymas dėl direktyvos
32 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	3. Jeigu priežiūros institucija, kompetentinga pagal Reglamentą (ES) 2016/679, yra įsteigta kitoje valstybėje narėje nei kompetentinga institucija, kompetentinga institucija ***informuoja*** toje pačioje valstybėje narėje įsteigtą priežiūros instituciją.

Pakeitimas 274

Pasiūlymas dėl direktyvos
35 straipsnio 1 pastraipa

Komisijos siūlomas tekstas	*Pakeitimas*
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□.***	Komisija ***ne vėliau kaip … [42 mėnesiai po šios direktyvos įsigaliojimo dienos] ir po to kas 36 mėnesius*** 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. ***Tuo*** tikslu ir siekiant tolesnės pažangos vykdant strateginį ir operatyvinį bendradarbiavimą, Komisija atsižvelgia į Bendradarbiavimo grupės ir CSIRT tinklo ataskaitas apie patirtį, įgytą strateginiu ir operatyviniu lygmeniu. ***Kai būtina, prie ataskaitos pridedamas pasiūlymas dėl teisėkūros procedūra priimamo akto.***

Pakeitimas 275

Pasiūlymas dėl direktyvos
36 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. 18 straipsnio 6 dalyje ir 21 straipsnio 2 dalyje nurodyti įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami penkerių metų laikotarpiui nuo […]	2. 18 straipsnio 6 ***dalyje, 20 straipsnio 11a*** dalyje ir 21 straipsnio 2 dalyje nurodyti įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami penkerių metų laikotarpiui nuo […]

Pakeitimas 276

Pasiūlymas dėl direktyvos
36 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	3. Europos Parlamentas arba Taryba gali bet kada atšaukti 18 straipsnio 6 dalyje***, 20 straipsnio 11a 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.

Pakeitimas 277

Pasiūlymas dėl direktyvos
36 straipsnio 6 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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	6. Pagal 18 straipsnio 6 ***dalį, 20 straipsnio 11a*** 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

laikotarpis pratęsiamas dviem mėnesiais.	arba Tarybos iniciatyva šis laikotarpis pratęsiamas dviem mėnesiais.

Pakeitimas 278

Pasiūlymas dėl direktyvos
42 straipsnio 1 a pastraipa (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	Tačiau 39 ir 40 straipsniai taikomi nuo … [18 mėnesių po šio reglamento įsigaliojimo dienos].

Pakeitimas 279

Pasiūlymas dėl direktyvos
I priedo 2 punkto d papunkčio 2 įtrauka (nauja)

Komisijos siūlomas tekstas

Pakeitimas

2. Transportas	d) Kelių transportas	— ***Elektromobilių išmaniojo įkrovimo paslaugų operatoriai***

Pakeitimas 280

Pasiūlymas dėl direktyvos
II priedo lentelės 6 a eilutė (nauja)

Komisijos siūlomas tekstas

Pakeitimas

6a. Švietimas ir moksliniai tyrimai		— ***Aukštojo mokslo įstaigos ir mokslo tiriamosios įstaigos***

AIŠKINAMOJI DALIS

Pranešėjas nori, kad Europa taptų geriausia vieta gyventi ir vykdyti verslą.

Todėl pranešėjas palankiai vertina Direktyvą dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti (TIS 2), kuria pakeičiama pradinė TIS direktyva (TIS 1). Pasiūlyme atsižvelgiama į pasikeitusią kibernetinio saugumo grėsmės aplinką ir nustatomas minimalus priemonių suderinimas visoje ES.

Šiuo metu Europos policijos pajėgos vis labiau stengiasi susidoroti su staigiu elektroninių nusikaltimų incidentų skaičiaus didėjimu. Incidentai gali apimti su aukštosiomis technologijomis susijusius nusikaltimus, nusikaltimus pasinaudojant kibernetine erdve ir generalinio direktoriaus sukčiavimą, tačiau pranešėjas nori aiškiai pabrėžti agresyvų išpirkos reikalavimo programinę įrangą naudojančių grupuočių, įsilaužiančių į Europos taikinius ir juos šantažuojančių, plitimą, neatsižvelgiant į jų dydį ar apyvartą. Savo ruožtu priešiški nacionalinės valstybės subjektai daugiausia dėmesio skiria intelektinės nuosavybės vagystėms pramoniniu mastu, kurioms reikalingas atitinkamas atsakas.

Tačiau, anot ENISA, ES organizacijos skiria 41 proc. mažiau lėšų kibernetiniam saugumui nei analogiškos JAV institucijos. Be to, atsakomybės pagal BDAR baimė labai apsunkino dalijimąsi informacija tarp šalių ir šalių viduje. Tai akivaizdu tiek viešuosiuose, tiek privačiuose subjektuose, kurie bijo dalytis duomenimis. Todėl TIS 2 turi būti aišku, jog dalijimasis informacija yra būtinas, kad būtų laikomasi kibernetinio saugumo reikalavimų.

Bendras ES kibernetinio saugumo lygis yra labai svarbus vidaus rinkos veikimui. Aiškiai apibrėžti teisės aktai yra būtini, kad skirtingose valstybėse narėse veikiančioms įmonėms būtų taikomos tos pačios taisyklės. TIS 2 norima pašalinti netikrumą ir dabartinį aiškumo trūkumą.

Amžiuje, kai kibernetiniai nusikaltimai, šnipinėjimas ar sabotažo operacijos gali turėti pakopinį poveikį, TIS 2 pagrįstai gerokai išplečiama **taikymo sritis**. Į pasiūlymą įtraukti sektoriai, kurie anksčiau nebuvo laikomi esminiais ar svarbiais, tačiau juos tikrai tokiai laiko išpirkos reikalavimo programinę įrangą naudojančios gaujos ar tam tikros nacionalinės valstybės. Remiantis paslaugomis, kurias subjektai teikia visuomenei, jie yra suskirstyti į šias dvi teisines kategorijas: „esminiai“ ir „svarbūs“ subjektai. Pranešėjas pritaria Komisijos pasiūlymo užmojui ir mano, kad mokslinių tyrimų ir akademinės įstaigos turėtų būti įtrauktos į naują sektorių. Šios institucijos yra labai tikslinės, o jų intelektinė nuosavybė nusipelno apsaugos pagal TIS 2.

Įmonėms tenkanti administracinė našta ir **biurokratija** turi nuolat kelti susirūpinimą visiems teisės aktų leidėjams. Pranešėjas pritaria sprendimui neįtraukti labai mažų ir mažų įmonių. Be to, jis mano, kad TIS 2 turėtų būti ne tik sutelkiamas dėmesys į reikalavimų laikymąsi ir baudžiamąsias priemones, bet ir į teigiamas paskatas, pvz., teikti gaires ir pagalbą MVĮ, turinčioms konkrečių poreikių ir interesų, arba į laisvai siūlomas paslaugas, skirtas elektroninio pašto serverio ir svetainės konfigūravimui patikrinti. Tokiais pasiūlymais taip pat siekiama šiuo klausimu parodyti, kad vyriausybės turi būti orientuotos į paslaugas.

Pranešimai apie incidentus yra labai svarbūs kibernetiniam saugumui: jais galima užkirsti kelią kitiems tapti kibernetinio išpuolio aukomis. Pranešėjas nori paminėti, kad eidamas buvusias pareigas kibernetinio saugumo srityje jis dažnai pastebėjo, kad neįmanoma pranešti apie incidentą per 24 valandas. Paprastai šiame ankstyvame etape incidentas vis dar lieka neaiškus, kol vėliau paaiškėja. Pranešėjui siūlomas 24 valandų laikotarpis atrodo nepagrįstas, taip pat dėl to, kad ekspertų pastangos sutelkiamos į problemos sušvelninimą; pranešimas

šiame etape yra antrinės svarbos. Kibernetinis incidentas ir jo padariniai retai gerai suvokiami per 24 valandas, o dėl reikalavimo pranešti per 24 valandas gali būti teikiami neteisingi pranešimai, teikiama pernelyg daug pranešimų ir gali kilti dar daugiau painiavos. Be to, šie incidentai dažnai įvyksta per savaitgalį. Todėl pranešėjas siūlo šią direktyvą suderinti su kitais Sąjungos teisės aktais, pvz., GDPR, taip prailginant terminą iki 72 valandų.

Pranešėjo nuomone, nėra pageidautina nustatyti, kad **pranešimai apie galimus incidentus** būtų privalomi. Reikėtų skatinti savanorišką dalijimąsi informacija apie galimus incidentus ar vos neįvykusius incidentus, tačiau vidutinio dydžio ir dideliems subjektams per vieną dieną gali kilti dešimtys ar net šimtai didelių kibernetinių grėsmių. Pranešimo apie šiuos galimus incidentus prievolė taptų našta ir mažintų atsako veiksmingumą. Tai taip pat galėtų pakenkti valdžios institucijų, kurios turi kovoti su šiais pranešimais, veiksmingumui, pakenkiant pasitikėjimui ataskaitų teikimo sistema ir jų gebėjimu veikti įvykus tikriems incidentams.

Taip pat neturėtų būti privaloma **pranešti apie galimas kibernetines grėsmes** CSIRT ar kompetentingoms institucijoms. Atitikties ir atsakomybės reikalavimas atgrasys nuo grėsmių ieškotojų veiklos; esminės kibernetinio saugumo ekosistemos dalies. Be to, pasitaiko (rimtų) atvejų, kai būtų geriau pranešti apie grėsmę žvalgybos bendruomenei, kai ji priklauso jų kompetencijos sričiai, o ne TIS institucijoms.

Kibernetinio saugumo priemonės turėtų atitikti subjekto dydį ir kibernetinio saugumo riziką, su kuria jis susiduria. Todėl **priežiūra ir vykdymo užtikrinimas** turėtų būti proporcingi. Baudos ir baudžiamosios priemonės yra labai svarbios, jei TIS 2 teisės aktai bus veiksmingi, tačiau pranešėjas mano, kad teisės aktų leidėjai turėtų pabrėžti, kad yra eskalavimo pakopos, todėl tik po akivaizdaus aplaidumo reaguojant į pakartotinius įspėjimus vyresnioji vadovybė būtų pasirengusi pajusti įstatymo galią. **Kelią užkirsti dvigubai priežiūrai** rengiant konkretiems sektoriams skirtus teisės aktus yra svarbu ir subjektams, kurie patenka į TIS 2 ir konkretiems sektoriams skirtą sritį, pvz., DORA.

Pranešėjas ragina visas valstybes nares parengti **nacionalinę kibernetinio saugumo strategiją dėl aktyvios kibernetinės gynybos**. Europoje po incidento mums pavyko gerai koordinuoti veiksmus, tačiau žinių (viešųjų ir privačiųjų) apie kibernetines atakas kaupimas iki jiems įvykstant taip pat reiškia atsakomybę. Vien tik dalytis tomis žiniomis nepakanka; piliečiai ir subjektai tikisi, kad jų vyriausybės laikysis aktyvios pozicijos kibernetinio saugumo apsaugos klausimais. Valstybės narės turi inicijuoti pajėgumus, kuriais būtų galima sutrukdyti išpuoliams ir aktyviai užkirsti kelią jų atsiradimui.

Interneto pagrindui taip pat reikia dėmesio. teikiant DNS paslaugas reikia pasiūlyti klientams saugias ir privatumą užtikrinančias paslaugas. Tai dar nėra visuotinai priimta. Pranešėjas yra susirūpinęs dėl to, kad piliečiai, turintys savo DNS paslaugą nešiojamame kompiuteryje ar mažame serveryje namuose, patenka į Komisijos pasiūlymo taikymo sritį. Pranešėjas pageidauja, kad šie asmenys, kurie dažnai yra technologijas išmanantys asmenys, nebūtų įtraukti į šią direktyvą. Kita problema yra ta, kad šakninių vardų serverių operatoriai yra įtraukti į TIS 2 taikymo sritį. Kadangi internetas augo aštuntajame ir devintajame praėjusio amžiaus dešimtmetyje ir vėliau, šias paslaugas valdo geri ekspertai savanoriai. Kadangi ši paslauga nėra monetizuojama ir kadangi galima teigti, kad Vyriausybės neturėtų ją reguliuoti, pranešėjas mano, kad šakniniai serveriai **neturėtų būti įtraukti į taikymo sritį**.

Pranešėjo nuomone, labai svarbu stiprinti bendrą elektroninių ryšių tinklų ir paslaugų saugumą ir gerinti interneto vientisumą. Tai reiškia, kad visoje Europoje turėtų būti taikomi sąveikūs pasitikėjimu grindžiami metodai. Labai skatinama naudoti Europos DNS keitiklius, ypač daug dėmesio skiriant privatumui ir saugumui, taip pat fizinę interneto ir povandeninių

ryšių kabelių apsaugą. Todėl ši direktyva turėtų būti vertinama atsižvelgiant į visą kibernetinio saugumo strategijos paketą, kurį pradėjo Komisija: mums reikia saugesnio interneto pagrindo.

Be to, TIS 2 suteikiamas teisinis pagrindas **koordinuotam saugumo rizikos vertinimui**, kurį atlieka Bendradarbiavimo grupė. 5G priemonių rinkinys buvo panaudotas kaip puikus pavyzdys. Pranešėjas mano, kad šiais rizikos vertinimais galėtų būti labai pagerintas Sąjungos saugumas ir strateginis savarankiškumas, ir mano, kad šie rizikos vertinimai turėtų būti atliekami įvairioms IRT paslaugoms, sistemoms ar produktams. Krovinių skaitytuvai oro uostuose ir uostuose yra aiškus pavyzdys, kurį jis nori paminėti šiuo klausimu.

Nenumatyta, kad esminis dalijimasis informacija buvo labai apsunkintas ir turėtų būti tobulinamas. Pavyzdžiui: per pastaruosius metus policijos pajėgos atrado ir iššifravo išpirkos reikalavimo programinę įrangą naudojančių gaujų serverius, kuriuose kartais buvo milijonai aukų, ES ir už ES ribų. Policijos darbas yra dirbti su naujais atvejais, todėl tai leidžia CSIRT pasiekti tikslus ir sušvelninti kibernetinių grėsmių poveikį atskleista informacija šiuose serveriuose. Deja, dėl nepagrįstų suvokiamų teisinių kliūčių beveik nė vienai aukai nebuvo pranešta ar padedama. Todėl labai svarbu, kad TIS 2 būtų sukuriamas aiškus teisinis pagrindas tokioms grėsmėms sumažinti ir dalytis informacija ne tik ES viduje, bet ir su partneriais už ES ribų.

Išplėtus taikymo sritį, CSIRT turi pasirengti pasiūlyti **keičiamo masto ir automatizuotus sprendimus**, kuriais būtų galima greitai ir saugiai paskirstyti koordinuotą pažeidžiamumo atskleidimą, pranešimus apie incidentus ir grėsmių žvalgybą. Keitimosi informacija automatizavimas yra ne tik šios direktyvos išvestinė priemonė – tai yra jos esmė. Visų gerų TIS 2 pasiūlymo ketinimų sąlyga – suteikti **teisinį pagrindą CSIRT ir įmonėms dalytis duomenimis** su savo klientais, kolegomis ir valdžios institucijomis tiek ES, tiek už jos ribų.

Standartų ir sertifikavimo schemų naudojimas yra dar viena teigiama Komisijos pasiūlymo ypatybė. Sertifikavimas turėtų būti įmanomas verčiau taikant konkrečias Europos ir tarptautiniu mastu pripažintas sistemas, o ne nacionalines sistemas. Suderinimas turėtų būti tikslas; taisyklės, taikomos vienoje valstybėje narėje, turėtų būti panašios į taisykles, taikomas kitose valstybėse narėse.

TIS 2 pasiūlyme reikalaujama, kad ENISA parengtų ir tvarkytų Europos pažeidžiamumų registrą. Pranešėjas mano, kad pirmenybė turėtų būti teikiama **Europos pažeidžiamumų duomenų bazei**, o ne registrams. Yra mažai priežasčių padvigubinti tai, kas jau yra ir naudojama kibernetinio saugumo bendruomenėje kaip bendras standartas visose pasaulio dalyse. Dvigubinimu bus pasėta nesantaika ir painiava ekspertų bendruomenėje. Europos duomenų bazė, o ne registras, turėtų sverto poveikį CVE registrui; tai tarptautinių viešai žinomų kibernetinio saugumo pažeidžiamumų, naudojamų visame pasaulyje, įrašų sąrašas. Pranešėjas mano, kad ENISA turėtų atlikti svarbų naują vaidmenį CVE registre, kuris dabar dažniausiai yra įsteigtas JAV. Be to, reikėtų užkirsti kelią pastangų dubliavimui; pageidautinas rezultatas turėtų būti duomenų bazė, kurioje Europos organizacijoms būtų keliami unikalūs uždaviniai. Galiausiai, dar svarbiau, pranešėjas pabrėžia, kad ENISA labai svarbu turėti veikiančią infrastruktūrą ir procedūras, skirtas įslaptintai informacijai tvarkyti. Kibernetinis saugumas turėtų būti tvarkomas nuo neįslaptinto lygio iki (aukščiausio) slapto lygio.

WHOIS duomenys – autoritetingas domeno nuosavybės įrašas – yra vienintelė perspektyvi priemonė gauti informaciją, reikalingą nusikalstamiems subjektams nustatyti, grėsmę keliantiems subjektams stebėti, užkirsti kelią žaloms ir internetinei ekosistemai apsaugoti.

Kibernetinio saugumo bendruomenė remiasi jais, taip pat jie leidžia grėsmių tyrėjams medžioti priešininkus, kad piliečiai ir subjektai patys galėtų apsisaugoti nuo artėjančių grėsmių. Tai vienintelis patikimas atskaitomybės mechanizmas kitaip anonimiškame internete. Tačiau per pastaruosius trejus metus, įsigaliojus BDAR, WHOIS duomenys kai kurių subjektų laikomi atsakomybės klausimu. Deja, nepagrįstai ilgalaikė WHOIS duomenų naudojimo praktika buvo sustabdyta. Todėl pranešėjas savo pranešime dar kartą primena duomenų tvarkymo dėl kibernetinio saugumo priežasčių teisėtumą pagal BDAR, aiškiai norėdamas, kad WHOIS duomenimis vėl būtų dalijamasi.

Apskritai pranešėjas mano, kad TIS 2 yra būtinas žingsnis siekiant suderinti mūsų vidaus rinką ir pagerinti kibernetinį saugumą visoje ES.

15.10.2021

PILIEČIŲ LAISVIŲ, TEISINGUMO IR VIDAUS REIKALŲ KOMITETO NUOMONĖ

pateikta Pramonės, mokslinių tyrimų ir energetikos komitetui

dėl pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Nuomonės referentas(*): Lukas Mandl(*)
Susijusių komitetų procedūra. Darbo tvarkos taisyklių 57 straipsnis

TRUMPAS PAGRINDIMAS

Europos Parlamento ir Tarybos direktyvos pasiūlymas dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva)[2] yra platesnio Sąjungos lygmens iniciatyvų, kuriomis siekiama didinti viešųjų ir privačiųjų subjektų atsparumą grėsmėms, rinkinio dalis. Pasiūlymu siekiama pašalinti dabartinių teisės aktų spragas ir sudaryti sąlygas subjektams, kuriems jis taikomas, geriau reaguoti į Komisijos poveikio vertinime, kurio metu buvo plačiai konsultuojamasi su suinteresuotaisiais subjektais, įvardytas problemas. Šios problemos visų pirma apima padidėjusią vidaus rinkos skaitmenizaciją ir kintančią saugumo grėsmių aplinką.

Pasiūlymo teisinis pagrindas – SESV 114 straipsnis, t. y. vidaus rinka. Tačiau LIBE požiūriu svarbu atkreipti dėmesį į tai, kad pagal TIS 2 direktyvą tinklo ir informacinėms sistemoms nustatytomis priemonėmis siekiama ne tik užtikrinti tinkamą vidaus rinkos veikimą. **Direktyva taip pat turėtų padėti prisidėti prie bendro Sąjungos saugumo** *inter alia* padėdama išvengti skirtingo valstybių narių paveikumo įvairiai kibernetiniam saugumui kylančiai rizikai.

Šiuo tikslu labai svarbu **pašalinti dabartinius valstybių narių skirtumus**, kurie atsiranda dėl nevienodo valstybių narių įstatymų aiškinimo. Dėl šios priežastis pranešėjas palankiai vertina reglamentu nustatytas vienodas sąlygas, siekiant nustatyti subjektus, kuriems taikoma direktyva. Papildomi pasiūlymai teikiami siekiant užkirsti kelią skirtingam įgyvendinimui, visų pirma siekiant įpareigoti Komisiją priimti gaires dėl *lex specialis* įgyvendinimo ir MVĮ taikomų kriterijų (kuriais taip pat turėtų būti užtikrinamas teisinis aiškumas ir išvengiama nereikalingos naštos), ir reikalauti, kad Bendradarbiavimo grupė nustatytų papildomus ne techninio pobūdžio veiksnius, į kuriuos reikia atsižvelgti atliekant tiekimo grandinės rizikos vertinimus. Be to, pažymėta, kad kompetentingos valdžios institucijos valstybėse narėse ir

[2] 2020/0359(COD)

tarp valstybių narių turi bendradarbiauti tikruoju laiku.

Pranešimo projekte taip pat atsižvelgiama į įvairias **EDAPP rekomendacijas**, kurias jis **pateikė** savo nuomonėje dėl kibernetinio saugumo strategijos ir TIS 2.0 direktyvos[3]. Svarbiausia tai, kad teksto konstatuojamosiose dalyse ir dėstomojoje dalyje patikslinama, kad bet koks asmens duomenų tvarkymas pagal TIS 2 direktyvą nedaro poveikio Reglamentui (ES) 2016/679 (BDAR)[4] ir Direktyvai 2002/58/EB[5] (e. Privatumo direktyva). Atsižvelgiant į siauresnę sąvokos „tinklų ir informacinių sistemų saugumas“ taikymo sritį (taikoma tik technologijos apsaugai), palyginti su „kibernetiniu saugumu“ (taip pat apima naudotojų apsaugos veiklą), pirmasis terminas naudojamas tik tais atvejais, kai tekstas yra išimtinai techninio pobūdžio. Atsižvelgiant į domeno vardus ir registracijos duomenis, siūlomi patikslinimai dėl 1) „atitinkamos informacijos“ paskelbimo tapatybės nustatymo ir susisiekimo tikslais teisinio pagrindo, 2) skelbiamų domeno registracijos duomenų kategorijų (remiantis Interneto vardų ir numerių paskyrimo korporacijos (ICANN) rekomendacija) ir 3) subjektų, kurie galėtų būti laikomi „teisėtais prieigos prašytojais“. Teisiniame tekste taip pat nurodyta, kad pasiūlymas nedaro poveikio duomenų priežiūros institucijų jurisdikcijos ir kompetencijos priskyrimui pagal BDAR. Galiausiai numatytas išsamesnis teisinis pagrindas, susijęs su pasiūlyme nurodytų kompetentingų institucijų ir kitų atitinkamų priežiūros institucijų, visų pirma priežiūros institucijų pagal BDAR, bendradarbiavimu ir keitimusi atitinkama informacija.

Kiti pakeitimai, kuriuos dėl Komisijos pasiūlymo pateikė LIBE pranešėjas, yra susiję su toliau išvardytais aspektais.

- Siekiant užtikrinti TIS 2 direktyvos ir pasiūlytos Direktyvos dėl ypatingos svarbos infrastruktūros subjektų atsparumo[6] nuoseklumą, kai kurių nuostatų kalba buvo suderinta su pasiūlymo dėl ypatingos svarbos subjektų nuostatomis. Laikantis panašaus pokyčio, numatyto Ypatingos svarbos subjektų direktyvoje, kuri turėtų būti taikoma tiems patiems sektoriams kaip ir TIS 2 direktyva, į taikymo sritį siūloma įterpti „maisto gamybą, perdirbimą ir platinimą“.
- Dėl asmens duomenų patikslinama, kad reagavimo į kompiuterių saugumo incidentus tarnybos (CSIRT) atliekamas tinklų ir informacinių sistemų skenavimas turėtų būti nesuderinamas ne tik su Reglamentu (ES) 2016/679 (BDAR)[7], bet ir Direktyva 2002/58/EB[8] (e. Privatumo direktyva). Tarptautiniai asmens duomenų perdavimai

[3] Nuomonė Nr. 5/2021: https://edps.europa.eu/system/files/2021-03/21-03-11_edps_nis2-opinion_en.pdf.
[4] 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) (Tekstas svarbus EEE) (*OL L 119, 2016 5 4, p. 1–88*).

[5] 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. 37–47*).

[6] 2020/0365(COD).
[7] 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) (Tekstas svarbus EEE) (*OL L 119, 2016 5 4, p. 1–88*).

[8] 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. 37–47*).

pagal šią direktyvą turėtų atitikti BDAR V skyrių.

- Bendradarbiavimo grupė turėtų susitikti veikiau du kartus per metus, o ne vieną kartą, kad įvertintų pokyčius kibernetinio saugumo srityje. Bendradarbiavimo grupės posėdžiuose EDAV dalyvauja stebėtojos teisėmis.
- ENISA turėtų per metus priimti vieną, o ne dvi kibernetinio saugumo būklės Sąjungoje ataskaitas. Ataskaitoje turėtų būti atsižvelgta į kibernetinio saugumo incidentų poveikį asmens duomenų apsaugai Sąjungoje.
- Terminas pranešimams apie incidentus suderinamas su terminu, per kurį pranešama apie BDAR pažeidimus, t. y. 72 valandos.
- Nors esminiai ir svarbūs subjektai apie faktinius kibernetinio saugumo incidentus turėtų pranešti privaloma tvarka, pranešimas apie kibernetines grėsmes turėtų būti savanoriškas, siekiant riboti administracinę naštą ir išvengti perteklinio pranešimų teikimo. Kad būtų laikomas reikšmingu, incidentas turėjo sukelti faktinę žalą ir nuo jo turėjo nukentėti kiti fiziniai ir juridiniai asmenys, o ne apsiribojama vien tokios žalos arba nukentėjimo galimybe.
- Aplinkybės, į kurias atsižvelgiama priimant sprendimą dėl sankcijos pažeidus kibernetinio saugumo taisykles, yra suderinamus su BDAR. Kadangi tai prieštarautų dabartinei atsakomybės praktikai pagal Sąjungos teisę, neturėtų būti įmanoma nustatyti laikino draudimo fiziniams asmenims įgyvendinti valdymo funkcijų.
- Siekiant išvengti žalos reputacijai, subjektai neturėtų būti įpareigoti viešai skelbti reikalavimų pagal šią direktyvą nesilaikymo aspektų arba už pažeidimą atsakingų fizinių ar juridinių asmenų tapatybės.

PAKEITIMAI

Piliečių laisvių, teisingumo ir vidaus reikalų komitetas ragina atsakingą Piliečių laisvių, teisingumo ir vidaus reikalų komitetą atsižvelgti į šiuos pakeitimus:

Pakeitimas 1

Pasiūlymas dėl direktyvos
1 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(1) Europos Parlamento ir Tarybos direktyva (ES) 2016/114811 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 Sąjungos ***saugumo ir veiksmingo***

visuomenės veikimo;

[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).

ekonomikos ir visuomenės ***veikimo***;

[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).

Pakeitimas 2

Pasiūlymas dėl direktyvos
2 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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 laimėjimų, peržiūrėjus Direktyvą (ES) 2016/1148 paaiškėjo jos trūkumai, trukdantys veiksmingai spręsti dabartines ir naujas kibernetinio saugumo problemas;	(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 ir sukuriant nacionalinių reagavimo į kompiuterinius saugumo incidentus tarnybų tinklą (CSIRT tinklas). Nepaisant šių laimėjimų, peržiūrėjus Direktyvą (ES) 2016/1148 paaiškėjo jos trūkumai, trukdantys veiksmingai spręsti dabartines ir naujas kibernetinio saugumo problemas; ***Be to, dėl COVID-19 pandemijos išsiplėtus internetinei veiklai išryškėjo kibernetinio saugumo, kuris yra itin svarbus ES piliečiams, kad jie galėtų pasitikėti inovacijomis ir junglumu, taip pat didelio masto švietimu ir mokymu***

šioje srityje svarba. Todėl Komisija turėtų padėti valstybėms narėms rengti švietimo programas kibernetinio saugumo srityje, kad svarbūs ir esminiai subjektai galėtų įdarbinti kibernetinio saugumo ekspertus, kurie galėtų vykdyti šioje direktyvoje nustatytus įsipareigojimus;

[12] Direktyvos (ES) 2016/1148 11 straipsnis.

[13] Direktyvos (ES) 2016/1148 12 straipsnis.

[12] Direktyvos (ES) 2016/1148 11 straipsnis.

[13] Direktyvos (ES) 2016/1148 12 straipsnis.

Pakeitimas 3

Pasiūlymas dėl direktyvos
3 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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***;***	(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***,*** padaryti didelę žalą Sąjungos ekonomikai***, mūsų demokratijos veikimui*** ir ***vertybėms bei laisvėms, kuriomis remiasi mūsų visuomenė***. Todėl kibernetinio saugumo parengtis ir veiksmingumas kaip niekad anksčiau yra labai svarbūs ***Sąjungos saugumui ir*** tinkamam vidaus rinkos veikimui ***, atsižvelgiant į kasdienės veiklos skaitmeninę transformaciją visoje***

	Sąjungoje. Tam reikia glaudesnio valstybių narių institucijų atskiro ir tarpusavio bendradarbiavimo, taip pat nacionalinių valdžios institucijų ir atsakingų Sąjungos įstaigų bendradarbiavimo.

Pakeitimas 4

Pasiūlymas dėl direktyvos
5 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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. ***Galiausiai dėl šių skirtumų kai kurios valstybės narės gali tapti labiau paveikios kibernetinio saugumo grėsmėms, įskaitant šalutinį poveikį visoje Sąjungoje, jos vidaus rinkos ir bendro saugumo atžvilgiu.*** 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, įskaitant ***valstybių narių kompetentingų institucijų tarpusavio bendradarbiavimą***, ***tikruoju laiku*** 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;

Pakeitimas 5

Pasiūlymas dėl direktyvos
6 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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];	(6) ši direktyva nedaro poveikio valstybių narių galimybei imtis priemonių, būtinų gyvybiniams jos ***nacionalinio*** saugumo interesams užtikrinti, viešajai tvarkai palaikyti bei visuomenės saugumui užtikrinti, ir sudaryti sąlygas ***užkardyti,*** 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];
[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).	[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).

Pakeitimas 6

Pasiūlymas dėl direktyvos
8 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(8) pagal Direktyvą (ES) 2016/1148 valstybės narės turėjo pareigą nustatyti, kurie subjektai atitinka esminių paslaugų	(8) ***valstybių narių pareiga*** pagal Direktyvą (ES) 2016/1148 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;

operatoriams taikomus kriterijus (nustatymo procesas) šiuo atžvilgiu ***lėmė*** didelius valstybių narių skirtumus. ***Nedarant poveikio konkrečioms šioje direktyvoje numatytoms išimtims,*** turėtų būti nustatytas vienas kriterijus, kuriuo remiantis nustatomi subjektai, kurie patenka į šios direktyvos taikymo sritį***, siekiant pašalinti šiuos skirtumus ir užtikrinti teisinį tikrumą dėl visiems subjektams taikomų rizikos valdymo reikalavimų ir pareigų pranešti***. 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;

---

[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).

[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).

Pakeitimas 7

Pasiūlymas dėl direktyvos
8 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(8a) Atsižvelgiant į nacionalinių viešojo administravimo sistemų skirtumus, valstybės narės išlaiko savo kompetenciją priimti sprendimus dėl subjektų, kuriems taikoma ši direktyva, skyrimo.

Pakeitimas 8

Pasiūlymas dėl direktyvos
9 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(9) į šios direktyvos taikymo sritį taip pat turėtų patekti mažieji arba labai maži subjektai, atitinkantys tam tikrus kriterijus, iš kurių matyti, kad jie***, remiantis rizikos vertinimu, įskaitant subjektus, kurie pagal Europos Parlamento ir Tarybos direktyvą (ES) XXX/XXX[1a] apibrėžiami kaip ypatingos svarbos subjektai arba jiems lygiaverčiai subjektai***, 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;
	_____
	[1a] Europos Parlamento ir Tarybos direktyva (ES) ***[XXX/XXX] dėl ypatingos svarbos subjektų atsparumo (OL...).***

Pakeitimas 9

Pasiūlymas dėl direktyvos
10 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(10) Komisija, bendradarbiaudama su Bendradarbiavimo grupe, gali paskelbti labai mažoms ir mažosioms įmonėms taikomų kriterijų įgyvendinimo gaires;	(10) Komisija, bendradarbiaudama su Bendradarbiavimo grupe, ***turėtų*** paskelbti labai mažoms ir mažosioms ***įmonėms*** taikomų kriterijų įgyvendinimo gaires;

Pakeitimas 10

Pasiūlymas dėl direktyvos
12 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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 ***turėtų*** 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;

Pakeitimas 11

Pasiūlymas dėl direktyvos
14 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(14) atsižvelgiant į kibernetinio saugumo ir subjektų fizinio saugumo tarpusavio ryšius, ***kai įmanoma ir tinkama,*** reikėtų užtikrinti nuoseklų požiūrį tarp Europos Parlamento ir Tarybos direktyvos (ES) XXX/XXX17 ir šios direktyvos. Kad pasiektų šį tikslą, valstybės narės turėtų užtikrinti, kad ypatingos svarbos subjektai pagal

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 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;

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 pagal Direktyvą (ES) XXX/XXX ***kompetentingų institucijų*** veikla ***valstybėse narėse ir tarp valstybių narių*** dalijantis informacija apie ***kibernetinius*** incidentus bei kibernetines grėsmes ir vykdant priežiūros užduotis. Institucijos pagal abi direktyvas turėtų bendradarbiauti ir keistis informacija ***valstybėse narėse ir tarp valstybių narių***, 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 ***dėl*** ypatingos svarbos ***subjektų pagal šią direktyvą ėmėsi kompetentingos institucijos***. Pagal Direktyvą (ES) XXX/XXX kompetentingų institucijų prašymu pagal šią direktyvą kompetentingoms institucijoms turėtų būti leidžiama ***įvertinti*** subjektų, kurie įvardijami kaip ypatingos svarbos subjektai, ***kibernetinį saugumą***. Šiuo tikslu abi institucijos turėtų bendradarbiauti ir keistis informacija ***tikruoju laiku***;

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

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

Pakeitimas 12

Pasiūlymas dėl direktyvos
18 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(18) duomenų centro paslaugų teikėjų siūlomos paslaugos ne visada gali būti teikiamos debesijos kompiuterijos	(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;	paslaugos forma. Atitinkamai, duomenų centrai ne visada gali priklausyti debesijos kompiuterijos infrastruktūrai. Siekiant valdyti visą riziką, kuri kyla ***kibernetiniam*** 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;

Pakeitimas 13

Pasiūlymas dėl direktyvos
20 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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, ***maisto gamybos, perdirbimo ir platinimo,*** 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

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;	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 pandemijos ***metu padažnėję išpuoliai prieš informacines sistemas*** parodė, kad mūsų vis labiau tarpusavyje priklausoma visuomenė yra pažeidžiama atsižvelgiant į mažai tikėtiną riziką; ***Todėl reikia papildomų investicijų į kibernetinį saugumą.***

Pakeitimas 14

Pasiūlymas dėl direktyvos
20 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(20a) Labai svarbu didinti kibernetinį sąmoningumą ir kibernetinį atsparumą visuose ypatingos svarbos ir esminiuose subjektuose, įskaitant viešojo administravimo subjektus.

Pakeitimas 15

Pasiūlymas dėl direktyvos
21 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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;

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 ***ir užtikrinti, kad ši institucija turi pakankamai išteklių veiksmingai ir efektyviai vykdyti savo pareigas***;

Pakeitimas 16

Pasiūlymas dėl direktyvos
22 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(22) siekiant palengvinti tarpvalstybinį institucijų bendradarbiavimą ir ryšių palaikymą bei sudaryti sąlygas veiksmingai įgyvendinti šią direktyvą, būtina, kad kiekviena valstybė narė paskirtų nacionalinį bendrąjį informacinį centrą, atsakingą už klausimų, susijusių su tinklų ir informacinių sistemų saugumu, koordinavimą ir tarpvalstybinį bendradarbiavimą Sąjungos lygmeniu;	(22) siekiant palengvinti tarpvalstybinį institucijų bendradarbiavimą ir ryšių palaikymą bei sudaryti sąlygas veiksmingai įgyvendinti šią direktyvą, būtina, kad kiekviena valstybė narė paskirtų nacionalinį bendrąjį informacinį centrą, atsakingą už klausimų, susijusių su ***kibernetiniu*** saugumu, koordinavimą ir tarpvalstybinį bendradarbiavimą Sąjungos lygmeniu;

Pakeitimas 17

Pasiūlymas dėl direktyvos
23 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(23) kompetentingos institucijos arba CSIRT turėtų veiksmingai ir efektyviai iš subjektų gauti pranešimus apie incidentus. Bendriesiems informaciniams centrams turėtų būti pavesta ***tikruoju laiku*** persiųsti pranešimus apie incidentus ***visų*** kitų 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;	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;

Pakeitimas 18

Pasiūlymas dėl direktyvos
25 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(25) kalbant apie asmens duomenis pažymėtina, kad CSIRT turėtų turėti galimybę pagal Europos Parlamento ir Tarybos Reglamentą (ES) 2016/679[19] ***ir Direktyvą 2005/58/EB*** subjekto vardu ir jo prašymu pagal šią direktyvą imtis iniciatyvos atlikti ***tinklo aprėpties ir*** informacinių sistemų, naudojamų jų paslaugoms teikti, saugumo skenavimą, ***siekiant nustatyti, sumažinti ir užkirsti kelią konkrečioms grėsmėms***. 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; ***Be to, kibernetinio saugumo rizika niekada neturėtų būti naudojama kaip pretekstas pažeisti pagrindines žmogaus teises;***
[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).	[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).

Pakeitimas 19

Pasiūlymas dėl direktyvos
27 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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 agentūros turėtų bendradarbiauti techniniu, operatyviniu ir politiniu lygmenimis, kad tinkamai koordinuotų atsaką visoje Sąjungoje;	(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, ***arba kelti rimtą pavojų visuomenės saugumui keliose valstybėse narėse arba visoje Sąjungoje***. Atsižvelgiant į tai, kad tokie incidentai yra labai įvairaus masto ir dažniausiai tarpvalstybinio pobūdžio, valstybės narės ir atitinkamos ES institucijos, įstaigos ir agentūros turėtų bendradarbiauti techniniu, operatyviniu ir politiniu lygmenimis, kad tinkamai koordinuotų atsaką visoje Sąjungoje; ***Valstybės narės turėtų stebėti, kaip įgyvendinamos ES taisyklės, teikti tarpusavio paramą iškilus bet kokioms tarpvalstybinėms problemoms, užmegzti labiau struktūrizuotą dialogą su privačiuoju sektoriumi ir bendradarbiauti sprendžiant saugumo ir grėsmių, susijusių su naujomis technologijomis, klausimus, kaip antai 5G technologijos atveju;***
[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).	[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).

Pakeitimas 20

Pasiūlymas dėl direktyvos
33 konstatuojamoji dalis

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

Pakeitimas 21

Pasiūlymas dėl direktyvos
34 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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);	(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 ***pakviesti*** jos veikloje dalyvauti kibernetinio saugumo politiką įgyvendinančias Sąjungos įstaigas ir agentūras, pavyzdžiui, ***visų pirma Europolą***, Europos Sąjungos aviacijos saugos agentūrą (EASA) ir Europos Sąjungos kosmoso programos agentūrą (EUSPA);

Pakeitimas 22

Pasiūlymas dėl direktyvos
36 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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. ***Trečiajai šaliai arba tarptautinei organizacijai perduodant asmens duomenis,*** turėtų būti ***taikomas Reglamento (ES) 2016/679 V skyriaus;***

Pakeitimas 23

Pasiūlymas dėl direktyvos
37 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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;	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 dviem ar daugiau valstybių narių ir įtariama, kad ji yra baudžiamojo pobūdžio, reikėtų apsvarstyti galimybę aktyvuoti ES Teisėsaugos institucijų reagavimo į ekstremalias situacijas protokolą.*** 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;

Pakeitimas 24

Pasiūlymas dėl direktyvos
45 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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 ***ir pranešti apie bet kokius galimus kibernetinius išpuolius, kuriuos jie nustato;***

Pakeitimas 25

Pasiūlymas dėl direktyvos
46 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(46a) Ypač reikėtų atsižvelgti į tai, kad IRT paslaugos, sistemos ar produktai, kuriems kilmės šalyje taikomi konkretūs reikalavimai, gali tapti kliūtimi laikytis ES privatumo ir duomenų apsaugos teisės aktų. Kai tinkama, atliekant tokius rizikos vertinimus reikėtų konsultuotis su Europos duomenų apsaugos valdyba (EDAV); laisvo naudojimo ir atvirojo kodo programinė įranga, taip pat atvirojo kodo aparatinė įranga galėtų suteikti milžiniškos naudos kibernetinio saugumo srityje, ypač kalbant apie skaidrumą ir galimybę patikrinti savybes. Kadangi tai padeda panaikinti ir mažinti konkrečias grėsmes tiekimo grandinei, kai įmanoma, reikėtų teikti pirmenybę jų naudojimui, vadovaujantis Europos duomenų apsaugos priežiūros pareigūno nuomone 5/2021[1a];
	[1a] Europos duomenų apsaugos priežiūros pareigūno nuomonė 5/2021 dėl kibernetinio saugumo strategijos ir TIS 2.0 direktyvos, 2021 m. kovo 11 d.

Pakeitimas 26

Pasiūlymas dėl direktyvos
47 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(47) atliekant tiekimo grandinės rizikos vertinimus, atsižvelgiant į atitinkamo sektoriaus ypatumus, turėtų būti atsižvelgiama tiek į techninius, tiek, kai tinkama, į netechninius veiksnius, ***kuriuos Bendradarbiavimo grupė turėtų apibūdinti išsamiau ir kurie apima***

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;	***veiksnius,*** 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;

Pakeitimas 27

Pasiūlymas dėl direktyvos
48 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(48a) mažosios ir vidutinės įmonės (MVĮ) dažnai yra per mažo masto ir joms stinga išteklių, kad patenkintų užsienio ir vis įvairesnius kibernetinio saugumo poreikius tarpusavyje sujungtame pasaulyje didėjant nuotolinio darbo mastui. Todėl valstybės narės savo nacionalinėse kibernetinio saugumo strategijose turėtų spręsti gairių ir paramos MVĮ klausimus;

Pakeitimas 28

Pasiūlymas dėl direktyvos
50 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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 ***kibernetinio*** 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;

Pakeitimas 29

Pasiūlymas dėl direktyvos
52 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(52) kai tinkama, subjektai turėtų ***turėti galimybę*** 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;

Pakeitimas 30

Pasiūlymas dėl direktyvos
53 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(53) visų pirma viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai turėtų ***įgyvendinti pritaikytojo ir standartizuotojo saugumo priemones ir sugebėti*** informuoti paslaugų gavėjus apie konkrečias ir dideles kibernetines grėsmes ir priemones, kurių jie gali imtis savo ***prietaisų ir*** ryšių saugumui užtikrinti, pavyzdžiui, naudodami konkrečių rūšių programinę įrangą arba šifravimo technologijas. ***Siekiant padidinti aparatinės ir programinės įrangos saugumą, paslaugų teikėjus reikėtų skatinti naudoti atvirojo kodo ir atvirąją aparatinę įrangą;***

Pakeitimas 31

Pasiūlymas dėl direktyvos
54 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(54) siekiant užtikrinti elektroninių ryšių tinklų ir paslaugų saugumą, ***taip pat pagrindines teises į duomenų apsaugą ir į privatumą,*** 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 ***pareiga*** užtikrinti savo esminių saugumo interesų apsaugą ir visuomenės saugumą ir leisti ***užkardyti***, atskleisti nusikalstamas veikas ir vykdyti baudžiamąjį persekiojimą už jas laikantis Sąjungos ***ir nacionalinės*** teisės. Sprendimai, susiję su teisėta prieiga prie

privatumą ir saugumą, ***kartu užtikrinant veiksmingą atsaką į nusikalstamumą***;	informacijos ištisiniuose šifruotuose ryšiuose, turėtų išlaikyti šifravimo veiksmingumą apsaugant ryšių privatumą ir saugumą***; Neturėtų būti laikoma, kad kuria nors šio reglamento nuostata siekiama supaprastinti ištisinį šifravimą taikant apėjimo būdus ar panašius sprendimus, nes šifravimo trūkumai gali būti panaudoti kenkėjiškiems tikslams. Bet kokia priemonė, kuria siekiama susilpninti šifravimą arba apeiti technologijos struktūrą, gali kelti didelę riziką jos apsaugos pajėgumų veiksmingumui. Neleistiną iššifravimą arba elektroninių ryšių stebėseną, kurią vykdo ne teisėtos valdžios institucijos, reikėtų uždrausti, siekiant užtikrinti technologijos veiksmingumą ir platesnį naudojimą. Svarbu, kad valstybės narės spręstų problemas, su kuriomis susiduria teisės institucijos ir pažeidžiamumo tyrėjai. Kai kuriose valstybėse narėse subjektams ir fiziniams asmenims, kurie tiria pažeidžiamumą, taikoma baudžiamoji ir civilinė atsakomybė. Todėl valstybės narės raginamos parengti gaires, kad dėl informacinio saugumo srities tyrimų nebūtų patraukiama baudžiamojon atsakomybėn ir vykdomas persekiojimas.***

Pakeitimas 32

Pasiūlymas dėl direktyvos
56 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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;	incidentus teikimą, valstybės narės turėtų sukurti vieną bendrą prieigą, 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 ***ir Europos duomenų apsaugos valdyba***, turėtų parengti bendrus pranešimo šablonus, pateikdama gaires, kuriomis būtų supaprastinta ir racionalizuota pagal Sąjungos teisę reikalaujama pranešimų teikimo informacija ir sumažinta bendrovėms tenkanti našta;

Pakeitimas 33

Pasiūlymas dėl direktyvos
57 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(57) kai įtariama, kad incidentas yra susijęs su sunkia nusikalstama veika pagal Sąjungos arba nacionalinę teisę, valstybės narės ***turėtų*** skatinti ***ir pranešti*** esminius ir svarbius subjektus, remiantis Sąjungos teisę atitinkančiomis taikytinomis baudžiamojo proceso taisyklėmis, 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 ***Europolo Europos kovos su elektroniniu nusikalstamumu centro (EC3)*** ir ENISA;

Pakeitimas 34

Pasiūlymas dėl direktyvos
58 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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 ***Reglamentą (ES) 2016/679 ir*** Direktyvą 2002/58/EB;

Pakeitimas 35

Pasiūlymas dėl direktyvos
59 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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 ***taikomus*** Sąjungos duomenų apsaugos teisės aktus;

Pakeitimas 36

Pasiūlymas dėl direktyvos
62 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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***	(62) ***siekiant laikytis teisinės pareigos pagal Reglamento (ES) 2016/679 6 straipsnio 1 dalies c punktą ir 6 straipsnio 3 dalį, aukščiausio*** lygio domenų vardų registrai ir jiems skirtas domenų vardų registravimo paslaugas teikiantys subjektai turėtų viešai skelbti ***tam tikrus*** domenų vardų registracijos duomenis, ***nurodytus valstybės narės teisėje, kuri jiems taikoma***,

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;

pavyzdžiui, ***domeno vardas ir juridinio asmens pavadinimas***. Aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys aukščiausio lygio domenų vardų registravimo paslaugas, ***atsižvelgdami į savo įgaliojimus,*** taip pat turėtų suteikti teisėtą prieigą prie fizinių asmenų konkrečių domenų vardų registracijos duomenų***, visų pirma pagal šią direktyvą kompetentingoms institucijoms arba Reglamente (ES) 2016/679 nurodytoms priežiūros institucijoms***. Valstybės narės turėtų užtikrinti, kad aukščiausio lygio domenų vardų registrai ir ***subjektai, teikiantys*** domenų vardų registravimo paslaugas***, gavę teisėtus ir tinkamai pagrįstus viešojo sektoriaus institucijų, įskaitant kompetentingas institucijas pagal šią direktyvą, kompetentingas institucijas pagal Sąjungos ar nacionalinę teisę nusikalstamų veikų prevencijos, tyrimo ar baudžiamojo persekiojimo už jas tikslais arba priežiūros institucijas pagal Reglamentą (ES) 2016/679, nepagrįstai nedelsdami atsakytų į*** 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;

---

[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“.

Pakeitimas 37

Pasiūlymas dėl direktyvos
63 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(63) ***taikant šią direktyvą***, 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 ***susitarti dėl klientų klasifikacijos, kai įmanoma,*** bendradarbiauti, ***tikruoju laiku*** teikti viena kitai savitarpio pagalbą ir prireikus vykdyti bendrus priežiūros veiksmus;

Pakeitimas 38

Pasiūlymas dėl direktyvos
64 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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. ***Taikant šią direktyvą,*** jurisdikcija turėtų būti priskirta valstybei narei, kurioje yra atitinkamo

Sąjungoje. Šioje direktyvoje įsisteigimo kriterijus reiškia 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;	subjekto pagrindinė buveinė Sąjungoje. Šioje direktyvoje įsisteigimo kriterijus reiškia 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;

Pakeitimas 39

Pasiūlymas dėl direktyvos
69 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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, ***yra būtinas siekiant laikytis savo teisinių įsipareigojimų pagal nacionalinės teisės aktus, kuriais perkeliama ši direktyva, todėl jam taikomas Reglamento (ES) 2016/679 6 straipsnio 1 dalies c punktas 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;

6 straipsnio 3 dalis. Be to, toks tvarkymas turėtų būti teisėtas atitinkamo duomenų valdytojo interesas, kaip nurodyta ***Reglamento*** (ES) 2016/679 ***6 straipsnio 1 dalies f punkte***. 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. ***Daugeliu atvejų asmens duomenų saugumui kyla pavojus įvykus kibernetiniams incidentams, todėl ES valstybių narių kompetentingos institucijos ir duomenų apsaugos institucijos turėtų bendradarbiauti ir keistis informacija visais susijusiais klausimais, kad būtų užkirstas kelias bet kokiems asmens duomenų saugumo pažeidimams.*** Taikant tokias priemones gali prireikti tvarkyti ***tam tikrų kategorijų*** asmens duomenis***, įskaitant*** IP adresus, universaliuosius išteklių adresus (URL), domenų vardus ir e. pašto adresus;

Pakeitimas 40

Pasiūlymas dėl direktyvos
71 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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 rimtumą ir trukmę,

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;	faktiškai padarytą žalą ar patirtus nuostolius arba galimą žalą ar nuostolius, kurie galėjo būti patirti***, bet kokius ankstesnius pažeidimus, pranešimo apie pažeidimą kompetentingai institucijai būdą***, 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. ***Nustatant*** 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;

Pakeitimas 41

Pasiūlymas dėl direktyvos
74 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(74) valstybės narės turėtų galėti nustatyti taisykles dėl baudžiamųjų sankcijų už nacionalinių taisyklių, kuriomis ši direktyva perkeliama į nacionalinę teisę, pažeidimus. ***Tomis baudžiamosiomis sankcijomis taip pat gali būti leidžiama konfiskuoti pelną, gautą pažeidus šį reglamentą.*** 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;

Pakeitimas 42

Pasiūlymas dėl direktyvos
76 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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. 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 ***veiksmingas teismines teisių gynimo priemones***, tinkamą procesą, nekaltumo prezumpciją ir teisę į gynybą;

Pakeitimas 43

Pasiūlymas dėl direktyvos
77 konstatuojamoji dalis

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

Pakeitimas 44

Pasiūlymas dėl direktyvos
79 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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***. ES turėtų padėti koordinuotai spręsti didelio masto kibernetinius incidentus ir krizes bei teikti pagalbą, kad būtų galima lengviau atsigauti po tokių kibernetinių išpuolių;***

Pakeitimas 45

Pasiūlymas dėl direktyvos
82 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(82a) ši direktyva netaikoma Sąjungos institucijoms, tarnyboms, įstaigoms ir agentūroms. Tačiau pagal šią direktyvą Sąjungos įstaigos galėtų būti laikomos esminiais arba svarbiais subjektais. Kad būtų pasiektas vienodas apsaugos lygis

taikant nuoseklias ir vienodas taisykles, Komisija iki 2022 m. gruodžio 31 d. turėtų paskelbti pasiūlymą dėl teisėkūros procedūra priimamo akto, kuriuo Sąjungos institucijos, tarnybos, įstaigos ir agentūros būtų įtrauktos į ES masto kibernetinio saugumo sistemą;

Pakeitimas 46

Pasiūlymas dėl direktyvos
84 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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,	(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 ***ir visapusiškai laikantis galiojančių Sąjungos teisės aktų, kuriais reguliuojami šie klausimai. Bet kokiam asmens duomenų tvarkymui pagal šią direktyvą taikomas Reglamentas (ES) 2016/679 ir Direktyva 2005/58/EB, atsižvelgiant į jų atitinkamas taikymo sritis, įskaitant priežiūros institucijų, turinčių kompetenciją stebėti šių teisinių priemonių laikymąsi, užduotis ir įgaliojimus,***

Pakeitimas 47

Pasiūlymas dėl direktyvos
2 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
1. Ši direktyva taikoma viešiesiems ir privatiesiems subjektams, kurie I priede įvardijami kaip esminiai subjektai, o II	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].

priede – kaip svarbūs subjektai. Ši direktyva netaikoma subjektams, kurie atitinka labai mažų ir mažųjų įmonių apibrėžtį pagal Komisijos rekomendaciją 2003/361/EB[28]. ***Komisijos rekomendacijos 2003/361/EB priedo 3 straipsnio 4 dalis netaikoma.***

[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).

[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).

Pakeitimas 48

Pasiūlymas dėl direktyvos
2 straipsnio 2 dalies įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. Tačiau, nepaisant subjektų dydžio, ši direktyva taikoma I ir II prieduose nurodytiems subjektams, kai:	2. Tačiau, nepaisant subjektų dydžio ***ir remiantis rizikos vertinimu pagal 18 straipsnį***, ši direktyva taikoma I ir II prieduose nurodytiems subjektams, kai:

Pakeitimas 49

Pasiūlymas dėl direktyvos
2 straipsnio 2 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
c) subjektas yra vienintelis paslaugos teikėjas ***valstybėje narėje***;	c) subjektas yra vienintelis paslaugos teikėjas ***nacionaliniu ar regioniniu lygmeniu***;

Pakeitimas 50

Pasiūlymas dėl direktyvos
2 straipsnio 2 dalies d punktas

Komisijos siūlomas tekstas	*Pakeitimas*
d) ***potencialus*** paslaugos, kurią teikia subjektas, sutrikimas galėtų turėti poveikį viešajam saugumui, visuomenės saugumui	d) paslaugos, kurią teikia subjektas, sutrikimas galėtų turėti poveikį viešajam saugumui, visuomenės saugumui arba

arba visuomenės sveikatai;

visuomenės sveikatai;

Pakeitimas 51

Pasiūlymas dėl direktyvos
2 straipsnio 2 dalies e punktas

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

Pakeitimas 52

Pasiūlymas dėl direktyvos
2 straipsnio 4 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	4a. Bet koks asmens duomenų tvarkymas pagal šią direktyvą atitinka Reglamentą (ES) 2016/679 ir Direktyvą 2002/58/EB ir apima tik tai, kas tikrai būtina ir proporcinga šios direktyvos taikymo tikslais.

Pakeitimas 53

Pasiūlymas dėl direktyvos
2 straipsnio 5 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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	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 ***yra būtina keitimosi tikslui pasiekti***. Keičiantis informacija saugomas tos informacijos konfidencialumas, ir esminių

konfidencialumas, ir esminių arba svarbių subjektų saugumo ir komerciniai interesai.

arba svarbių subjektų saugumo ir komerciniai interesai.

Pakeitimas 54

Pasiūlymas dėl direktyvos
2 straipsnio 6 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	6a. Komisija iki 2021 m. gruodžio 31 d. paskelbia pasiūlymą dėl teisėkūros procedūra priimamo akto į bendrą ES masto kibernetinio saugumo sistemą įtraukti Sąjungos institucijas, tarnybas, įstaigas ir agentūras, siekiant nuosekliomis ir vienodomis taisyklėmis užtikrinti vienodą apsaugos lygį.

Pakeitimas 55

Pasiūlymas dėl direktyvos
4 straipsnio 1 pastraipos 1 punkto b papunktis

Komisijos siūlomas tekstas	*Pakeitimas*
b) bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba	b) bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis ***ir kurie yra integruoti į IT sistemą ir naudojami numatytoms paslaugoms teikti***, grupė arba

Pakeitimas 56

Pasiūlymas dėl direktyvos
4 straipsnio 1 pastraipos 4 punktas

Komisijos siūlomas tekstas	*Pakeitimas*
(4) nacionalinė kibernetinio saugumo strategija – nuosekli valstybės narės sistema, kurioje nustatyti tos valstybės narės ***tinklų ir informacinių sistemų*** saugumo strateginiai tikslai ir prioritetai;	(4) nacionalinė kibernetinio saugumo strategija – nuosekli valstybės narės sistema, kurioje nustatyti tos valstybės narės ***kibernetinio*** saugumo strateginiai tikslai ir prioritetai;

Pakeitimas 57

Pasiūlymas dėl direktyvos
4 straipsnio 1 pastraipos 12 punktas

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	***Išbraukta.***

Pakeitimas 58

Pasiūlymas dėl direktyvos
4 straipsnio 1 pastraipos 22 punktas

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	***Išbraukta.***

Pakeitimas 59

Pasiūlymas dėl direktyvos
4 straipsnio 1 pastraipos 24 punktas

Komisijos siūlomas tekstas	*Pakeitimas*
(24) subjektas – bet kuris fizinis asmuo arba juridinis asmuo, įsteigtas ir tokiu pripažintas pagal jo įsteigimo vietos	*(Tekstas lietuvių kalba nekeičiamas.)*

nacionalinę teisę, kuris, veikdamas savo vardu, įgyvendina teises ir kuriam gali būti taikomos pareigos;

Pakeitimas 60

Pasiūlymas dėl direktyvos
5 straipsnio 1 dalies a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) valstybių narių kibernetinio saugumo strategijos tikslų ir prioritetų apibrėžtis;	a) valstybių narių kibernetinio saugumo strategijos tikslų ir prioritetų apibrėžtis***, atsižvelgiant į bendrą piliečių informuotumo apie kibernetinį saugumą lygį ir bendrą vartotojų susietųjų įrenginių saugumo lygį***;

Pakeitimas 61

Pasiūlymas dėl direktyvos
5 straipsnio 1 dalies f punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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 ***valstybėse narėse ir tarp jų*** siekiant dalytis informacija apie incidentus bei kibernetines grėsmes ir vykdyti priežiūros užduotis.
[38] [įrašyti visą pavadinimą ir OL paskelbimo nuorodą, kai ji bus žinoma]	[38] [įrašyti visą pavadinimą ir OL paskelbimo nuorodą, kai ji bus žinoma]

Pakeitimas 62

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*

b) gaires dėl su kibernetiniu saugumu susijusių reikalavimų, taikomų IRT produktams ir paslaugoms viešuosiuose pirkimuose, ir tokių reikalavimų specifikacijų;	b) gaires dėl su kibernetiniu saugumu susijusių reikalavimų, taikomų IRT produktams ir paslaugoms viešuosiuose pirkimuose, ir tokių reikalavimų specifikacijų***, įskaitant šifravimo reikalavimus ir atvirųjų šaltinių kibernetinio saugumo produktų naudojimo skatinimą, bet tuo neapsiribojant***;

Pakeitimas 63

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies d a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	da) politiką, susijusią su tolesniu atvirųjų duomenų ir atvirųjų šaltinių naudojimu saugumui skaidrumo priemonėmis užtikrinti;

Pakeitimas 64

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies d b punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	db) politiką, kuria skatinamas internetinių paslaugų naudotojų privatumas ir asmens duomenų saugumas;

Pakeitimas 65

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies e punktas

Komisijos siūlomas tekstas	*Pakeitimas*
e) politiką dėl kibernetinio saugumo įgūdžių skatinimo, informuotumo didinimo ir mokslinių tyrimų ir technologinės plėtros iniciatyvų;	e) politiką dėl kibernetinio saugumo įgūdžių skatinimo, informuotumo didinimo ir mokslinių tyrimų ir technologinės plėtros iniciatyvų***, įskaitant kibernetinio saugumo mokymo programų rengimą, kad subjektai būtų aprūpinti specialistais ir***

	technikais;

Pakeitimas 66

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies f punktas

Komisijos siūlomas tekstas	*Pakeitimas*
f) politiką dėl ***akademinių*** ir mokslinių tyrimų ***institucijų rėmimo siekiant tobulinti*** kibernetinio saugumo priemones ir saugią tinklų infrastruktūrą;	f) politiką dėl ***paramos akademinėms*** ir mokslinių tyrimų ***institucijoms, kurios prisideda prie nacionalinės kibernetinio saugumo strategijos kuriant ir diegiant*** kibernetinio saugumo priemones ir saugią tinklų infrastruktūrą***, kuria prisidedama prie nacionalinės kibernetinio saugumo strategijos, įskaitant konkrečią politiką, kuria sprendžiami su lyčių atstovavimu ir pusiausvyra šiame sektoriuje susiję klausimai***;

Pakeitimas 67

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies h punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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 ***ir jų gebėjimą reaguoti į kibernetinio saugumo incidentus***.

Pakeitimas 68

Pasiūlymas dėl direktyvos
6 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. ENISA sukuria ir tvarko Europos	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.	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. ***Siekdama užtikrinti registre esančios informacijos saugumą ir prieinamumą, ENISA taiko naujausias saugumo priemones ir pateikia informaciją kompiuterio skaitomu formatu per atitinkamas sąsajas.***

Pakeitimas 69

Pasiūlymas dėl direktyvos
7 straipsnio 3 dalies a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) nacionalinių pasirengimo priemonių ir veiksmų tikslai;	a) nacionalinių ***ir, kai tinkama ir taikytina, regioninių ir tarpvalstybinių*** pasirengimo priemonių ir veiksmų tikslai;

Pakeitimas 70

Pasiūlymas dėl direktyvos
10 straipsnio 2 dalies e punktas

Komisijos siūlomas tekstas	*Pakeitimas*
e) subjekto prašymu ***aktyviai*** patikrina	e) subjekto prašymu patikrina

tinklų ir ***informacines sistemas, kurias subjektas naudoja teikdamas*** paslaugas;	***informacinių sistemų*** ir ***tinklo aprėpties, naudojamų subjektui teikiant*** paslaugas***, saugumą, kad nustatytų, sumažintų ar užkardytų specifines grėsmes***; ***atliekant tokį patikrinimą tvarkomi tik tie asmens duomenys, kurie yra tikrai būtini, ir bet kuriuo atveju – IP adresai ir URL;***

Pakeitimas 71

Pasiūlymas dėl direktyvos
11 straipsnio 4 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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 ***pagal jų atitinkamas kompetencijas***.
[39] [įrašyti visą pavadinimą ir OL paskelbimo nuorodą, kai ji bus žinoma]	[39] [įrašyti visą pavadinimą ir OL paskelbimo nuorodą, kai ji bus žinoma]

Pakeitimas 72

Pasiūlymas dėl direktyvos
11 straipsnio 5 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
5. Valstybės narės užtikrina, kad jų kompetentingos institucijos reguliariai teiktų informaciją pagal Direktyvą	5. Valstybės narės užtikrina, kad jų kompetentingos institucijos reguliariai ***laiku*** teiktų informaciją pagal Direktyvą

(ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva] paskirtoms kompetentingoms institucijoms apie kibernetinio 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.	(ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva] paskirtoms kompetentingoms institucijoms apie kibernetinio 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.

Pakeitimas 73

Pasiūlymas dėl direktyvos
12 straipsnio 3 dalies įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	3. Bendradarbiavimo grupę sudaro valstybių narių, Komisijos ir ENISA atstovai. Europos išorės veiksmų tarnyba***, Europolo Europos kovos su elektroniniu nusikalstamumu centras ir Europos duomenų apsaugos valdyba*** Bendradarbiavimo grupėje dalyvauja ***stebėtojo*** teisėmis. Europos priežiūros institucijos (EPI) pagal Reglamento (ES) XXXX/XXXX [DORA reglamentas] 17 straipsnio 5 dalies c punktą gali dalyvauti Bendradarbiavimo grupės veikloje.

Pakeitimas 74

Pasiūlymas dėl direktyvos
12 straipsnio 3 dalies 1 pastraipa

Komisijos siūlomas tekstas	*Pakeitimas*
Prireikus Bendradarbiavimo grupė ***gali pakviesti*** atitinkamų suinteresuotųjų šalių atstovus dalyvauti jos darbe.	Bendradarbiavimo grupė***, kai tai yra svarbu vykdant jos užduotis, pakviečia*** atitinkamų suinteresuotųjų šalių atstovus dalyvauti jos darbe***, o Europos Parlamentą***

– dalyvauti stebėtojo teisėmis.

Pakeitimas 75

Pasiūlymas dėl direktyvos
12 straipsnio 8 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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 ***palengvintų*** strateginį bendradarbiavimą ir keitimąsi informacija ***realiuoju laiku***.

Pakeitimas 76

Pasiūlymas dėl direktyvos
13 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	2. CSIRT tinklą sudaro valstybių narių CSIRT ir CERT-EU atstovai. Komisija ***ir Europolo Europos kovos su elektroniniu nusikalstamumu centras*** dalyvauja CSIRT tinklo veikloje ***stebėtojo*** teisėmis. ENISA teikia sekretoriato paslaugas ir aktyviai remia CSIRT tarpusavio bendradarbiavimą.

Pakeitimas 77

Pasiūlymas dėl direktyvos
14 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	2. „EU-CyCLONe“ sudaro valstybių narių krizių valdymo institucijų, paskirtų pagal 7 straipsnį, Komisijos ir ENISA atstovai. ***Europolo Europos kovos su elektroniniu nusikalstamumu centras dalyvauja „EU-CyCLONe“ veikloje stebėtojo teisėmis.*** ENISA teikia tinklo

	sekretoriato paslaugas ir padeda saugiai keistis informacija.

Pakeitimas 78

Pasiūlymas dėl direktyvos
14 straipsnio 6 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
6. „EU-CyCLONe“ su CSIRT tinklu bendradarbiauja remdamasis sutartomis procedūrinėmis taisyklėmis.	6. „EU-CyCLONe“ su CSIRT tinklu bendradarbiauja remdamasis sutartomis procedūrinėmis taisyklėmis***, o su teisėsaugos institucijomis – pagal ES teisėsaugos institucijų reagavimo į ekstremaliąsias situacijas protokolą***.

Pakeitimas 79

Pasiūlymas dėl direktyvos
15 straipsnio 1 dalies įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
1. ENISA, bendradarbiaudama su Komisija, ***kas dvejus metus*** rengia kibernetinio saugumo Sąjungoje būklės ataskaitą. ***Ataskaitoje*** visų pirma įvertinami šie aspektai:	1. ENISA, bendradarbiaudama su Komisija, rengia ***metinę*** kibernetinio saugumo Sąjungoje būklės ataskaitą. ***Ataskaita pateikiama kompiuterio skaitomu formatu ir joje*** visų pirma įvertinami šie aspektai:

Pakeitimas 80

Pasiūlymas dėl direktyvos
15 straipsnio 1 dalies c a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ca) kibernetinio saugumo incidentų poveikis asmens duomenų apsaugai Sąjungoje;

Pakeitimas 81

Pasiūlymas dėl direktyvos
15 straipsnio 1 dalies c b punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	cb) piliečių bendro informuotumo apie kibernetinį saugumą ir naudojimo lygio, taip pat bendro vartotojams skirtų susietųjų įrenginių, pateiktų Sąjungos rinkai, saugumo lygio apžvalga.

Pakeitimas 82

Pasiūlymas dėl direktyvos
17 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	2. Valstybės narės užtikrina, kad valdymo organo nariai ***ir už kibernetinį saugumą atsakingi specialistai*** reguliariai dalyvautų specialiuose mokymuose, kad įgytų pakankamai žinių ir įgūdžių, kad galėtų suprasti ir įvertinti ***kintančią*** kibernetinio saugumo riziką ir valdymo praktiką bei jos poveikį subjekto veiklai.

Pakeitimas 83

Pasiūlymas dėl direktyvos
18 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	1. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai imtųsi tinkamų ir proporcingų techninių ir organizacinių priemonių, siekdami valdyti tinklų ir informacinių sistemų, ***naudojamų jų paslaugoms teikti, kibernetiniam*** saugumui kylančią riziką***, taip pat užtikrinti šių paslaugų tęstinumą ir sumažinti riziką, keliamą asmenų teisėms, kai tvarkomi jų asmens duomenys***. Remiantis naujausiais technikos laimėjimais, tomis priemonėmis turi būti užtikrinamas toks tinklų ir informacinių sistemų ***kibernetinio*** saugumo lygis, kuris

atitinka kylančią riziką.

Pakeitimas 84

Pasiūlymas dėl direktyvos
18 straipsnio 2 dalies g punktas

Komisijos siūlomas tekstas	*Pakeitimas*
g) kriptografijos ir šifravimo naudojimą.	g) kriptografijos ir ***sudėtingo*** šifravimo naudojimą.

Pakeitimas 85

Pasiūlymas dėl direktyvos
18 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	3. Valstybės narės užtikrina, kad, svarstydami 2 dalies d punkte nurodytas tinkamas ***ir proporcingas*** 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. ***Kompetentingos institucijos teikia subjektams gaires praktinio ir proporcingo taikymo klausimais.***

Pakeitimas 86

Pasiūlymas dėl direktyvos
18 straipsnio 6 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	6a. Valstybės narės suteikia tinklo ir informacinės sistemos, kurią teikia esminis ar svarbus subjektas, naudotojui teisę gauti iš subjekto informaciją apie technines ir organizacines priemones, kuriomis siekiama valdyti tinklų ir informacinių sistemų saugumui kylančią riziką. Valstybės narės nustato šios teisės apribojimus.

Pakeitimas 87

Pasiūlymas dėl direktyvos
19 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	1. Bendradarbiavimo grupė, bendradarbiaudama su Komisija ir ENISA, ***atlieka*** suderintus konkrečių ypatingos svarbos IRT paslaugų, sistemų ar produktų tiekimo grandinių saugumo rizikos vertinimus, atsižvelgdama į techninius ir, kai tinkama, netechninius rizikos veiksnius.

Pakeitimas 88

Pasiūlymas dėl direktyvos
20 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	1. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai nepagrįstai nedelsdami ***ir bet kuriuo atveju per 24 valandas*** praneštų kompetentingoms institucijoms arba CSIRT pagal 3 ir 4 dalis apie bet kokį incidentą, turintį didelį poveikį jų paslaugų teikimui***, ir kompetentingoms teisėsaugos institucijoms, jei įtariama arba žinoma***, ***kad incidentas yra piktavališko pobūdžio.*** Tie subjektai nepagrįstai nedelsdami ***ir bet kuriuo atveju per 24 valandas*** praneša jų paslaugų gavėjams apie incidentus, kurie gali turėti neigiamos įtakos tos paslaugos teikimui***, ir teikia informaciją, kuri jiems leistų sušvelninti neigiamą kibernetinių incidentų poveikį. Išimties tvarka, jei viešas informacijos atskleidimas galėtų sukelti papildomų kibernetinių incidentų, tie subjektai gali apie tai pranešti vėliau***. Valstybės narės užtikrina, kad tie subjektai, be kita ko, praneštų visą informaciją, pagal kurią kompetentingos institucijos arba CSIRT galėtų nustatyti tarpvalstybinį

incidento poveikį.

Pakeitimas 89

Pasiūlymas dėl direktyvos
20 straipsnio 2 dalies įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	2. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai ***galėtų pranešti*** kompetentingoms institucijoms arba CSIRT apie bet kokią didelę kibernetinę grėsmę, kurią tie subjektai nustatė ir dėl kurios galėtų įvykti didelis incidentas.

Pakeitimas 90

Pasiūlymas dėl direktyvos
20 straipsnio 2 dalies 1 pastraipa

Komisijos siūlomas tekstas	*Pakeitimas*
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.	Kai taikytina, ***tiems subjektams leidžiama pranešti*** 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. ***Kai daromas toks pranešimas,*** subjektai taip pat praneša tiems gavėjams apie pačią grėsmę. Dėl pranešimo pranešančiojo subjekto atsakomybė nepadidėja.

Pakeitimas 91

Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies c punkto įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
c) ne vėliau kaip per vieną mėnesį nuo a punkte nurodytos ataskaitos pateikimo – ***galutinę*** ataskaitą, kurioje pateikiama bent	c) ne vėliau kaip per vieną mėnesį nuo a punkte nurodytos ataskaitos pateikimo – ***išsamią*** ataskaitą, kurioje pateikiama bent

ši informacija:	ši informacija:

Pakeitimas 92

Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies c punkto ii papunktis

Komisijos siūlomas tekstas	*Pakeitimas*
ii) grėsmės arba pagrindinės priežasties, dėl kurios incidentas galėjo būti sukeltas, rūšį;	ii) grėsmės arba pagrindinės priežasties, dėl kurios ***kibernetinis*** incidentas galėjo būti sukeltas, rūšį;

Pakeitimas 93

Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies c punkto iii papunktis

Komisijos siūlomas tekstas	*Pakeitimas*
iii) taikomos ir įgyvendinamos poveikio mažinimo priemonės.	iii) taikomos ir įgyvendinamos poveikio mažinimo ***arba teisių gynimo*** priemonės.

Pakeitimas 94

Pasiūlymas dėl direktyvos
20 straipsnio 6 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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. ***Jei incidentas yra susijęs su dviem ar daugiau valstybių narių ir įtariama, kad jis yra nusikalstamo pobūdžio, kompetentinga institucija arba CSIRT apie tai informuoja Europolą.*** 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.

Pakeitimas 95

Pasiūlymas dėl direktyvos
22 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	2. ENISA, ***pasikonsultavusi su EDAV ir*** 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.

Pakeitimas 96

Pasiūlymas dėl direktyvos
23 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	1. Siekdamos prisidėti prie DNS saugumo, stabilumo ir atsparumo, valstybės narės užtikrina, kad ***būtų nustatyta*** aukščiausio lygio domenų vardų ***politika*** ir ***procedūros***, ***siekiant užtikrinti***, ***kad būtų renkami*** ir specialioje duomenų bazėje ***saugomi tikslūs*** ir ***išsamūs*** domenų vardų registracijos ***duomenys***, kuriems taikomi Sąjungos duomenų apsaugos teisės aktai dėl duomenų, kurie yra asmens duomenys. ***Valstybės narės užtikrina, kad tokia politika ir procedūros būtų skelbiamos viešai.***

Pakeitimas 97

Pasiūlymas dėl direktyvos
23 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	2. Valstybės narės užtikrina, kad 1 dalyje nurodytose domenų vardų registracijos duomenų bazėse būtų ***būtina*** informacija, pagal kurią būtų galima nustatyti domenų vardų turėtojus***, t. y. jų vardą ir pavardę ar pavadinimą, fizinį ir e. pašto adresą, taip pat jų telefono numerį,*** ir kontaktinius centrus, administruojančius aukščiausio lygio domenų vardais pažymėtus domenų vardus, ir su jais susisiekti.

Pakeitimas 98

Pasiūlymas dėl direktyvos
23 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	***Išbraukta.***

Pagrindimas

Ši dalis įtraukta į 23 straipsnio 1 dalį.

Pakeitimas 99

Pasiūlymas dėl direktyvos
23 straipsnio 4 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
4. Valstybės narės užtikrina, kad aukščiausio lygio domenų vardų registrai ir	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***.	subjektai, teikiantys domenų vardų registravimo paslaugas aukščiausio lygio domenų vardams, ***pagal Reglamento (ES) 2016/579 6 straipsnio 1 dalies c punktą ir 6 straipsnio 3 dalį ir*** nepagrįstai nedelsdami po domeno vardo užregistravimo paskelbtų ***tam tikrus*** domeno ***vardo*** registracijos duomenis, ***pavyzdžiui, domeno vardą ir juridinio*** asmens ***pavadinimą***.

Pakeitimas 100

Pasiūlymas dėl direktyvos
23 straipsnio 5 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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 ***viešojo sektoriaus institucijų, įskaitant kompetentingas institucijas pagal šią direktyvą, kompetentingas institucijas pagal Sąjungos ar nacionalinę teisę nusikalstamų veikų prevencijos, tyrimo ar baudžiamojo persekiojimo už jas tikslais arba priežiūros institucijas pagal Reglamentą (ES) 2016/679,*** 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 ***teisėtus ir tinkamai pagrįstus*** prašymus suteikti prieigą. Valstybės narės užtikrina, kad tokių duomenų atskleidimo politika ir procedūros būtų skelbiamos viešai.

Pakeitimas 101

Pasiūlymas dėl direktyvos
24 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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. ***Nedarant poveikio priežiūros institucijų kompetencijai pagal Reglamentą (ES) 2016/679,*** 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.

Pakeitimas 102

Pasiūlymas dėl direktyvos
25 straipsnio 1 dalies įžanginė dalis

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

Pakeitimas 103

Pasiūlymas dėl direktyvos
26 straipsnio 1 dalies įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
1. Nedarant poveikio Reglamentui (ES) 2016/679, valstybės narės užtikrina, kad esminiai ir svarbūs subjektai galėtų	1. Nedarant poveikio Reglamentui (ES) 2016/679 ***arba Direktyvai 2002/58/EB***, valstybės narės užtikrina, kad

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:	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, ***taip pat išpuolį vykdančio asmens buvimo vieta ir tapatybe,*** kai tokiu dalijimusi informacija:

Pakeitimas 104

Pasiūlymas dėl direktyvos
28 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. Kompetentingos institucijos, nagrinėdamos incidentus, dėl kurių pažeidžiamas asmens duomenų saugumas, glaudžiai bendradarbiauja su ***duomenų apsaugos institucijomis***.	2. Kompetentingos institucijos, nagrinėdamos incidentus, dėl kurių pažeidžiamas asmens duomenų saugumas, glaudžiai bendradarbiauja su ***priežiūros institucijomis, nepažeidžiant priežiūros institucijų kompetencijos, užduočių ir įgaliojimų pagal Reglamentą (ES) 2016/679. Šiuo tikslu kompetentingos institucijos ir priežiūros institucijos keičiasi informacija, kuri yra svarbi atsižvelgiant į jų atitinkamą kompetencijos sritį. Be to, kompetentingos institucijos, paprašius kompetentingoms priežiūros institucijoms, teikia joms visą informaciją, gautą atliekant bet kokius auditus ir tyrimus, susijusius su asmens duomenų tvarkymu.***

Pakeitimas 105

Pasiūlymas dėl direktyvos
29 straipsnio 4 dalies h punktas

Komisijos siūlomas tekstas	*Pakeitimas*
h) nurodyti tiems subjektams konkrečiu būdu viešai paskelbti šioje direktyvoje nustatytų pareigų nevykdymo	***Išbraukta.***

aspektus;

Pakeitimas 106

Pasiūlymas dėl direktyvos
29 straipsnio 5 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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.	***Išbraukta.***

Pakeitimas 107

Pasiūlymas dėl direktyvos
29 straipsnio 5 dalies 1 pastraipa

Komisijos siūlomas tekstas	*Pakeitimas*
Šios sankcijos taikomos tik tol, kol subjektas imasi būtinų veiksmų trūkumams pašalinti arba kompetentingos institucijos, kuriai taikytos tokios sankcijos, reikalavimams įvykdyti.	***Ši sankcija taikoma*** tik tol, kol subjektas imasi būtinų veiksmų trūkumams pašalinti arba kompetentingos institucijos, kuriai taikytos tokios sankcijos, reikalavimams įvykdyti.

Pakeitimas 108

Pasiūlymas dėl direktyvos
29 straipsnio 7 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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,	c) faktiškai padarytą ***turtinę ar neturtinę*** žalą ar patirtus nuostolius, jei juos galima nustatyti. Vertinant šį aspektą, be kita ko, atsižvelgiama į faktinius ar galimus finansinius ar ekonominius nuostolius, poveikį kitoms paslaugoms,

poveikį kitoms paslaugoms, paveiktų ar galimai paveiktų naudotojų skaičių;	paveiktų ar galimai paveiktų naudotojų skaičių;

Pakeitimas 109

Pasiūlymas dėl direktyvos
29 straipsnio 7 dalies c a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ca) bet kuriuos to atitinkamo subjekto svarbius ankstesnius pažeidimus;

Pakeitimas 110

Pasiūlymas dėl direktyvos
29 straipsnio 7 dalies c b punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	cb) tai, kokiu būdu kompetentinga institucija sužinojo apie pažeidimą, visų pirma tai, ar subjektas pranešė apie pažeidimą (jei taip – kokiu mastu);

Pakeitimas 111

Pasiūlymas dėl direktyvos
29 straipsnio 7 dalies g punktas

Komisijos siūlomas tekstas	*Pakeitimas*
g) ***atsakingu (-ais) laikomo (-ų) fizinio (-ų) ar juridinio (-ų) asmens (-ų)*** bendradarbiavimo su kompetentingomis institucijomis lygį***.***	g) bendradarbiavimo su kompetentingomis institucijomis***, siekiant ištaisyti pažeidimą ir sumažinti galimą neigiamą pažeidimų poveikį,*** lygį***;***

Pakeitimas 112

Pasiūlymas dėl direktyvos
29 straipsnio 7 dalies g a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ga) kitus sunkinančius ar švelninančius veiksnius, susijusius su konkretaus atvejo aplinkybėmis, pavyzdžiui, finansinę naudą, kuri buvo gauta, arba nuostolius, kurių buvo išvengta, tiesiogiai ar netiesiogiai dėl pažeidimo.

Pakeitimas 113

Pasiūlymas dėl direktyvos
29 straipsnio 9 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	9. Valstybės narės užtikrina, kad jų kompetentingos institucijos ***realiuoju laiku*** informuotų atitinkamas ***visų valstybių narių*** 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.

Pakeitimas 114

Pasiūlymas dėl direktyvos
30 straipsnio 4 dalies g punktas

Komisijos siūlomas tekstas	*Pakeitimas*
g) nurodyti tiems subjektams konkrečiu būdu viešai paskelbti šioje direktyvoje nustatytų pareigų nevykdymo aspektus;	***Išbraukta.***

Pakeitimas 115

Pasiūlymas dėl direktyvos
30 straipsnio 4 dalies h punktas

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

Pakeitimas 116

Pasiūlymas dėl direktyvos
31 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	2. Administracinės baudos 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***, priklausomai nuo kiekvienos atskiros bylos aplinkybių***.

Pakeitimas 117

Pasiūlymas dėl direktyvos
31 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
3. ***Sprendžiant***, ar skirti administracinę baudą, ir kiekvienu atskiru atveju priimant sprendimą dėl jos dydžio***,***	3. ***Sprendimas***, ar skirti administracinę baudą, ***priklauso nuo kiekvienos atskiros bylos aplinkybių,*** ir

deramai atsižvelgiama bent į 29 straipsnio 7 dalyje nurodytus aspektus.	kiekvienu atskiru atveju priimant sprendimą dėl jos dydžio deramai atsižvelgiama bent į 29 straipsnio 7 dalyje nurodytus aspektus.

Pakeitimas 118

Pasiūlymas dėl direktyvos
32 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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 informuoja priežiūros institucijas, kompetentingas pagal to reglamento 55 ir 56 straipsnius***, nepagrįstai nedelsdamos ir bet kuriuo atveju per 24 valandas***.

Pakeitimas 119

Pasiūlymas dėl direktyvos
32 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	3. Jeigu priežiūros institucija, kompetentinga pagal Reglamentą (ES) 2016/679, yra įsteigta kitoje valstybėje narėje nei kompetentinga institucija, kompetentinga institucija ***informuoja*** toje pačioje valstybėje narėje įsteigtą priežiūros instituciją.

Pakeitimas 120

Pasiūlymas dėl direktyvos
34 a straipsnis (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*

	34a straipsnis
	Atsakomybė už nuostatų nesilaikymą
	Nedarant poveikio jokioms turimoms administracinėms ar neteisminėms teisių gynimo priemonėms, esminių ir svarbių subjektų teikiamų paslaugų gavėjai, patyrę žalą dėl to, kad paslaugų teikėjai nesilaikė šios direktyvos, turi teisę į veiksmingą teisminę teisių gynimo priemonę.

Pakeitimas 121

Pasiūlymas dėl direktyvos
35 straipsnio 1 pastraipa

Komisijos siūlomas tekstas	*Pakeitimas*
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□.	Komisija ***kas trejus metus*** peržiūri šios direktyvos taikymą ir teikia ataskaitą Europos Parlamentui ir Tarybai. Ataskaitoje visų pirma įvertinama***, kokia apimtimi direktyva padėjo užtikrinti aukštą bendrą tinklų ir informacinių sistemų saugumo ir vientisumo lygį, kartu užtikrinant optimalią privataus gyvenimo ir asmens duomenų apsaugą,*** 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... □***36*** mėnesiai po šios direktyvos įsigaliojimo dienos□.

Pakeitimas 122

Pasiūlymas dėl direktyvos
I priedo 5 punkto („Sveikatos priežiūra“) 6 įtrauka (nauja)

Komisijos siūlomas tekstas

Sektorius	Pasektorius	Subjekto rūšis
5. Sveikatos priežiūra		– Sveikatos priežiūros paslaugų teikėjai, nurodyti Direktyvos 2011/24/ES[90] 3 straipsnio g punkte – ES etaloninės laboratorijos, nurodytos Reglamento XXXX/XXXX dėl didelių tarpvalstybinio pobūdžio grėsmių sveikatai[91] 15 straipsnyje – Subjektai, vykdantys vaistų, nurodytų Direktyvos 2001/83/EB[92] 1 straipsnio 2 punkte, mokslinių tyrimų ir kūrimo veiklą – Subjektai, gaminantys pagrindinius farmacijos produktus ir farmacijos preparatus, nurodytus NACE 2 red. C skirsnio 21 skyriuje – Subjektai, gaminantys medicinos priemones, kurios laikomos kritinėmis esant ekstremaliajai visuomenės sveikatai situacijai (toliau – ypatingos svarbos visuomenės sveikatai priemonių sąrašas), kaip nurodyta Reglamento XXXX[93] 20 straipsnyje

[91] [Europos Parlamento ir Tarybos reglamentas dėl didelių tarpvalstybinio pobūdžio grėsmių sveikatai, kuriuo panaikinamas Sprendimas Nr. 1082/2013/ES; nuoroda bus atnaujinta priėmus pasiūlymą COM(2020) 727 *final*]

[92] 2001 m. lapkričio 6 d. Europos Parlamento ir Tarybos direktyva 2001/83/EB dėl Bendrijos kodekso, reglamentuojančio žmonėms skirtus vaistus (OL L 311, 2001 11 28, p. 67).

[93] [Europos Parlamento ir Tarybos reglamentas dėl didesnio Europos vaistų agentūros vaidmens pasirengimo vaistų ir medicinos priemonių krizei ir jos valdymo srityje; nuoroda bus atnaujinta priėmus pasiūlymą COM(2020) 725 *final*]

Pakeitimas

Sektorius	Pasektorius	Subjekto rūšis
5. Sveikatos priežiūra		– Sveikatos priežiūros paslaugų teikėjai, nurodyti Direktyvos 2011/24/ES[90] 3 straipsnio g punkte – ES etaloninės laboratorijos, nurodytos Reglamento XXXX/XXXX dėl didelių tarpvalstybinio pobūdžio grėsmių sveikatai[91] 15 straipsnyje – Subjektai, vykdantys vaistų, nurodytų Direktyvos 2001/83/EB[92] 1 straipsnio 2 punkte, mokslinių tyrimų ir kūrimo veiklą – Subjektai, gaminantys pagrindinius farmacijos produktus ir farmacijos preparatus, nurodytus NACE

2 red. C skirsnio 21 skyriuje

– Subjektai, gaminantys medicinos priemones, kurios laikomos kritinėmis esant ekstremaliajai visuomenės sveikatai situacijai (toliau – ypatingos svarbos visuomenės sveikatai priemonių sąrašas), kaip nurodyta Reglamento XXXX[93] 20 straipsnyje

– Subjektai, turintys leidimą verstis vaistų didmenininko veikla, kaip nurodyta Direktyvos 2001/83/EB 79 straipsnyje

[91] [Europos Parlamento ir Tarybos reglamentas dėl didelių tarpvalstybinio pobūdžio grėsmių sveikatai, kuriuo panaikinamas Sprendimas Nr. 1082/2013/ES; nuoroda bus atnaujinta priėmus pasiūlymą COM(2020) 727 *final*]

[92] 2001 m. lapkričio 6 d. Europos Parlamento ir Tarybos direktyva 2001/83/EB dėl Bendrijos kodekso, reglamentuojančio žmonėms skirtus vaistus (OL L 311, 2001 11 28, p. 67).

[93] [Europos Parlamento ir Tarybos reglamentas dėl didesnio Europos vaistų agentūros vaidmens pasirengimo vaistų ir medicinos priemonių krizei ir jos valdymo srityje; nuoroda bus atnaujinta priėmus pasiūlymą COM(2020) 725 *final*]

NUOMONĘ TEIKIANČIO KOMITETO PROCEDŪRA

Pavadinimas	Priemonės aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, Direktyvos (ES) 2016/1148 panaikinimas
Nuorodos	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Atsakingas komitetas Paskelbimo plenariniame posėdyje data	ITRE 21.1.2021
Nuomonę pateikė Paskelbimo plenariniame posėdyje data	LIBE 21.1.2021
Susiję komitetai - paskelbimo plenariniame posėdyje data	20.5.2021
Nuomonės referentas (-ė) Paskyrimo data	Lukas Mandl 12.4.2021
Svarstymas komitete	16.6.2021 3.9.2021 11.10.2021
Priėmimo data	12.10.2021
Galutinio balsavimo rezultatai	+: 44 –: 14 0: 4
Posėdyje per galutinį balsavimą dalyvavę nariai	Magdalena Adamowicz, Katarina Barley, Pernando Barrena Arza, Pietro Bartolo, Nicolas Bay, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Patrick Breyer, Saskia Bricmont, Jorge Buxadé Villalba, Damien Carême, Caterina Chinnici, Clare Daly, Marcel de Graaff, Anna Júlia Donáth, Lena Düpont, Cornelia Ernst, Laura Ferrara, Nicolaus Fest, Maria Grapini, Sophia in ‘t Veld, Patryk Jaki, Marina Kaljurand, Assita Kanko, Fabienne Keller, Peter Kofod, Moritz Körner, Jeroen Lenaers, Juan Fernando López Aguilar, Lukas Mandl, Roberta Metsola, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Nicola Procaccini, Emil Radev, Paulo Rangel, Terry Reintke, Diana Riba i Giner, Ralf Seekatz, Michal Šimečka, Birgit Sippel, Sara Skyttedal, Martin Sonneborn, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Milan Uhrík, Tom Vandendriessche, Bettina Vollath, Elissavet Vozemberg-Vrionidi, Jadwiga Wiśniewska, Javier Zarzalejos
Posėdyje per galutinį balsavimą dalyvavę pavaduojantys nariai	Olivier Chastel, Tanja Fajon, Jan-Christoph Oetjen, Philippe Olivier, Anne-Sophie Pelletier, Thijs Reuten, Rob Rooken, Maria Walsh

GALUTINIS VARDINIS BALSAVIMAS NUOMONĘ TEIKIANČIAME KOMITETE

44	+
ID	Nicolas Bay, Nicolaus Fest, Peter Kofod, Philippe Olivier, Annalisa Tardino, Tom Vandendriessche
NI	Laura Ferrara
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Lena Düpont, Jeroen Lenaers, Lukas Mandl, Roberta Metsola, Nadine Morano, Emil Radev, Paulo Rangel, Ralf Seekatz, Sara Skyttedal, Elissavet Vozemberg-Vrionidi, Maria Walsh, Javier Zarzalejos
RENEW	Olivier Chastel, Anna Júlia Donáth, Sophia in 't Veld, Fabienne Keller, Moritz Körner, Jan-Christoph Oetjen, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu
S&D	Katarina Barley, Pietro Bartolo, Caterina Chinnici, Tanja Fajon, Maria Grapini, Marina Kaljurand, Juan Fernando López Aguilar, Javier Moreno Sánchez, Thijs Reuten, Birgit Sippel, Bettina Vollath
Verts/ALE	Damien Carême

14	-
ECR	Jorge Buxadé Villalba, Patryk Jaki, Assita Kanko, Nicola Procaccini, Rob Rooken, Jadwiga Wiśniewska
ID	Marcel de Graaff
NI	Martin Sonneborn, Milan Uhrík
Verts/ALE	Patrick Breyer, Saskia Bricmont, Terry Reintke, Diana Riba i Giner, Tineke Strik

4	0
The Left	Pernando Barrena Arza, Clare Daly, Cornelia Ernst, Anne-Sophie Pelletier

Sutartiniai ženklai:
+ : už
- : prieš
0 : susilaikė

15.6.2021

UŽSIENIO REIKALŲ KOMITETO NUOMONĖ

pateikta Pramonės, mokslinių tyrimų ir energetikos komitetui

dėl pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148
(2020/0359(COD))

Nuomonės referentė: Markéta Gregorová

PAKEITIMAI

Užsienio reikalų komitetas ragina atsakingą Pramonės, mokslinių tyrimų ir energetikos komitetą atsižvelgti į šiuos pakeitimus:

Pakeitimas 1

Pasiūlymas dėl direktyvos
2 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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]	(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 laimėjimų, peržiūrėjus Direktyvą (ES) 2016/1148 paaiškėjo jos trūkumai, trukdantys veiksmingai spręsti dabartines ir naujas kibernetinio saugumo problemas;

ir sukuriant nacionalinių reagavimo į kompiuterinius saugumo incidentus tarnybų tinklą (CSIRT tinklas)[13]***. Direktyva (ES) 2016/1148 buvo pirmasis Sąjungos masto teisėkūros procedūra priimtas aktas dėl kibernetinio saugumo, kuriame nustatytos teisinės priemonės bendram kibernetinio atsparumo lygiui didinti, be kita ko, saugumo ir gynybos srityje Sąjungoje, užtikrinant valstybių narių bendradarbiavimą ir saugumo kultūrą visuose sektoriuose***. Nepaisant šių laimėjimų, peržiūrėjus Direktyvą (ES) 2016/1148 paaiškėjo jos trūkumai, trukdantys veiksmingai spręsti dabartines ir naujas kibernetinio saugumo problemas***, kurios dažnai kyla už Sąjungos ribų, o tai kelia rimtą grėsmę vidaus ir išorės saugumui Sąjungos lygmeniu***;

[12] Direktyvos (ES) 2016/1148 11 straipsnis.

[13] Direktyvos (ES) 2016/1148 12 straipsnis.

[12] Direktyvos (ES) 2016/1148 11 straipsnis.

[13] Direktyvos (ES) 2016/1148 12 straipsnis.

Pakeitimas 2

Pasiūlymas dėl direktyvos
3 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(3a) Sąjunga mano, kad hibridinės kampanijos yra „daugialypės, jose derinamos prievartos ir provokavimo priemonės, naudojant tradicines ir netradicines priemones bei taktikas (diplomatines, karines, ekonomines ir technologines) siekiant destabilizuoti priešininką. Jos sukurtos taip, kad jas būtų sunku aptikti ar priskirti, ir jomis gali naudotis valstybiniai ir nevalstybiniai subjektai“[1a]. Internetas ir internetiniai tinklai leidžia valstybiniams ir nevalstybiniams subjektams imtis agresyvių veiksmų naujais būdais. Jie gali būti naudojami siekiant įsilaužti į

ypatingos svarbos infrastruktūrą ir įsiskverbti į demokratinius procesus, pradėti įtikinamas dezinformacijos ir propagandos kampanijas, pavogti informaciją ir įkelti neskelbtinus duomenis į viešąją erdvę. Blogiausiais atvejais kibernetiniai išpuoliai sudaro sąlygas priešininkui perimti tokių išteklių kaip karinės sistemos ir vadovavimo struktūros kontrolę[1b]. Tuo pat metu detalus bendradarbiavimas su privačiojo sektoriaus ir civiliais suinteresuotaisiais subjektais, įskaitant pramonės įmones ir subjektus, susijusius su ypatingos svarbos infrastruktūros objektų valdymu, yra labai svarbus ir turėtų būti stiprinamas dėl kibernetinei sričiai būdingų ypatumų, nes šioje srityje technologines inovacijas daugiausia skatina privačiojo sektoriaus įmonės, kurios dažnai neveikia karinėje srityje. Tokie didelio masto kibernetinio saugumo incidentams ir krizėms Sąjungos lygmeniu turėtų būti tinkamai pasirengta ir nuo jų apsisaugota, tuo tikslu rengiant bendras mokymo pratybas, nes dėl tokių incidentų ir krizių gali būti taikomas SESV 222 straipsnis (solidarumo sąlyga);

[1a] Europos Komisijos ir Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai bendras komunikatas dėl atsparumo ir pajėgumų didinimo kovojant su hibridinėmis grėsmėmis, JOIN(2018) 16 final, Briuselis, 2018 m. birželio 13 d., p. 1.

[1b] https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52018JC0016

Pakeitimas 3

Pasiūlymas dėl direktyvos
3 b konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(3b) kilus didelio masto kibernetinio

saugumo incidentams ir krizėms Sąjungos lygmeniu, dėl didelės sektorių ir šalių tarpusavio priklausomybės reikia imtis koordinuotų veiksmų, kad būtų užtikrintas greitas ir veiksmingas reagavimas, taip pat geresnė prevencija ir geresnis pasirengimas panašioms situacijoms ateityje. Siekiant užtikrinti Sąjungos saugumą jos viduje ir už jos ribų būtina turėti kibernetinėms grėsmėms atsparius tinklus ir informacines sistemas bei prieinamus, konfidencialius ir vientisus duomenis. Sąjungos siekis įgyti svarbesnį geopolitinį vaidmenį taip pat priklauso nuo patikimos kibernetinės gynybos ir atgrasymo, įskaitant gebėjimą laiku ir veiksmingai nustatyti kenkėjiškus veiksmus ir tinkamai į juos reaguoti. Atsižvelgiant į nykstančią ribą tarp civilinių ir karinių sričių, taip pat į dvejopą kibernetinių priemonių ir technologijų naudojimą, būtina laikytis visapusiško ir holistinio požiūrio į skaitmeninę sritį. Tas pats pasakytina apie operacijas ir misijas, kurias Sąjunga vykdo pagal bendrą saugumo ir gynybos politiką (BSGP), siekdama užtikrinti taiką ir stabilumą kaimyninėse šalyse ir už jų ribų. Šiuo atžvilgiu pagal ES strateginį kelrodį turėtų būti sustiprintas Sąjungos užmojų saugumo ir gynybos srityje įgyvendinimas ir bus padedama juos įgyvendinti, taip pat šie užmojai bus paversti pajėgumų poreikiais kibernetinės gynybos srityje, ir taip bus padidintas Sąjungos ir valstybių narių gebėjimas užkirsti kelią kibernetinei kenkimo veiklai, jai trukdyti, nuo jos atgrasyti, į ją reaguoti ir atsigauti po jos, stiprinant Sąjungos poziciją, informuotumą apie padėtį, priemones, procedūras ir partnerystes. ***Sąjungos bendradarbiavimas su tarptautinėmis organizacijomis, pavyzdžiui, NATO, prisideda prie diskusijų, kaip užkirsti kelią hibridiniams ir kibernetiniams išpuoliams, nuo jų atgrasyti ir į juos reaguoti, taip pat bendradarbiaujant ieškoma būdų, kaip parengti bendrą kibernetinių grėsmių***

analizę;

Pakeitimas 4

Pasiūlymas dėl direktyvos
6 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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];	(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 ***ir atsižvelgiant į pagrindines teises***. ***Nepaisant technologinių galimybių, turi būti visapusiškai paisoma tinkamo proceso ir kitų apsaugos priemonių, visų pirma pagrindinių teisių, būtent teisės į tai, kad būtų gerbiamas privatus gyvenimas bei komunikacijos slaptumas, ir teisės į asmens duomenų apsaugą. Taip pat mano, kad siekiant užtikrinti visapusišką atsparumą, būtina ne tik stiprinti technologinę infrastruktūrą ir turėti reagavimo pajėgumus, bet ir didinti visuomenės informuotumą apie kibernetines grėsmes ir saugumą.*** 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];
[14] Srauto kontrolės protokolas (TLP) – tai priemonė, kurią naudodamas kuris nors asmuo dalijasi informacija, kad informuotų	[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).	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).

Pakeitimas 5

Pasiūlymas dėl direktyvos
14 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(14a) siekiant kurti saugią junglumo sistemą ir remtis Europos kvantine ryšių infrastruktūra (EuroQCI) ir Europos Sąjungos vyriausybiniu palydoviniu ryšiu (GOVSATCOM), visų pirma įgyvendinant GALILEO GNSS gynybos naudotojams, o kartu ateityje vykdant bet kokią galimą plėtrą turėtų būti atsižvelgiama į poveikį, kurį lemia kvantinės kompiuterijos greičio ir sudėtingumo sujungimas su labai savarankiškomis karinėmis sistemomis, valstybės narės turėtų užtikrinti visos elektroninių ryšių infrastruktūros (kosmoso, sausumos ir povandeninių tinklų sistemos) apsaugą. Tuo pat metu reikėtų sukurti bendrą viziją dėl debesijos strategijos pažeidžiamuose sektoriuose, siekiant apibrėžti Sąjungos požiūrį, pagrįstą bendrais panašiai mąstančių valstybių partnerių standartais;

Pakeitimas 6

Pasiūlymas dėl direktyvos
20 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(20) šią didėjančią tarpusavio priklausomybę lemia vis labiau tarptautinio pobūdžio ir tarpusavyje priklausomas paslaugų teikimo tinklas, kuriame naudojami pagrindiniai visoje Sąjungoje	(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***;

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. ***Infrastruktūra, kaip kosmoso programų dalis, priklausanti Sąjungai ir valdoma arba eksploatuojama Sąjungos arba jos vardu, yra itin svarbi Sąjungos bei jos valstybių narių saugumo ir tinkamo BSGP misijų veikimo požiūriu. Tokia infrastruktūra turi būti tinkamai saugoma vadovaujantis Europos Parlamento ir Tarybos reglamentu (ES) Nr. 2021/696[18a].*** 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 ***ir kelti pavojų Sąjungos piliečių apsaugai ir saugumui***. COVID-19 pandemija parodė, kad mūsų vis labiau tarpusavyje priklausoma visuomenė yra pažeidžiama***, kai patiriama*** mažai ***tikėtina rizika***;

[18a] 2021 m. balandžio 28 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/696, kuriuo sudaroma Sąjungos kosmoso programa, įsteigiama Europos Sąjungos kosmoso programos agentūra ir panaikinami reglamentai (ES) Nr. 912/2010, (ES) Nr. 1285/2013 bei (ES) Nr. 377/2014 ir Sprendimas Nr. 541/2014/ES (OL L 170, 2021 5 12,

p. 69).

Pakeitimas 7

Pasiūlymas dėl direktyvos
26 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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***;***	(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***, kad galėtų prisidėti prie Sąjungos standartų, kurie gali formuoti kibernetinio saugumo aplinką tarptautiniu lygmeniu, rengimo. Valstybės narės taip pat galėtų išnagrinėti galimybę stiprinti bendradarbiavimą su panašių pažiūrų šalimis partnerėmis ir tarptautinėmis organizacijomis, pavyzdžiui, Europos Taryba, Šiaurės Atlanto sutarties organizacija, Ekonominio bendradarbiavimo ir plėtros organizacija, Europos saugumo ir bendradarbiavimo organizacija ir Jungtinėmis Tautomis, siekiant užtikrinti daugiašalius susitarimus dėl kibernetinių normų, atsakingą valstybinių ir nevalstybinių subjektų elgesį kibernetinėje erdvėje ir veiksmingą pasaulinį skaitmeninį valdymą, taip pat sukurti atvirą, laisvą, stabilią ir saugią kibernetinę erdvę, grindžiamą tarptautine teise;***

Pakeitimas 8

Pasiūlymas dėl direktyvos
27 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(27) pagal Komisijos rekomendacijos (ES) 2017/1548 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes (planas)[20] priedą	(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 agentūros turėtų bendradarbiauti techniniu, operatyviniu ir politiniu lygmenimis, kad tinkamai koordinuotų atsaką visoje Sąjungoje***;***	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, ***arba kelti pavojų piliečių apsaugai ir saugumui bei ekonominiams ir finansiniams Sąjungos interesams***. Atsižvelgiant į tai, kad tokie incidentai yra labai įvairaus masto ir dažniausiai tarpvalstybinio pobūdžio, valstybės narės ir atitinkamos ES institucijos, įstaigos ir agentūros turėtų bendradarbiauti techniniu, operatyviniu ir politiniu lygmenimis, kad tinkamai koordinuotų atsaką visoje Sąjungoje***.*** ***Sąjunga ir valstybės narės taip pat turėtų toliau skatinti pratybas ir scenarijais grindžiamas politines diskusijas dėl krizių valdymo sistemos, kad būtų užtikrintas vidaus ir išorės politikos nuoseklumas ir bendras supratimas apie solidarumo sąlygos įgyvendinimo procedūras;***
[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).	[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).

Pakeitimas 9

Pasiūlymas dėl direktyvos
36 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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***;***	organizuojamas. ***Tokiais susitarimais turi būti užtikrinta*** tinkama duomenų apsauga ***ir jais turėtų būti skatinamas patekimas į rinką, taip pat sprendžiamos saugumo rizikos problemos, kartu didinant pasaulinį atsparumą ir informuotumą apie kibernetines grėsmes ir kibernetinę kenkimo veiklą. Sąjunga taip pat turėtų toliau remti gebėjimų stiprinimą trečiosiose šalyse. Atitinkamais atvejais valstybės narės turėtų skatinti panašių pažiūrų šalis partneres, kurios vadovaujasi tokiomis pat vertybėmis kaip Sąjunga, dalyvauti atitinkamuose PESCO projektuose. Todėl Sąjunga turėtų išnagrinėti galimybę atnaujinti procesą, kuriuo siekiama ateityje sukurti oficialias ir struktūrizuotas bendradarbiavimo šioje srityje sistemas;***

Pakeitimas 10

Pasiūlymas dėl direktyvos
37 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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, ***Europos kovos su elektroniniu nusikalstamumu centrą ir ES žvalgybos ir situacijų centrą (EU INTCEN), siekdamos plėtoti strateginį žvalgybinį bendradarbiavimą kibernetinių grėsmių ir veiklos srityje, kad būtų toliau remiamas Sąjungos informuotumas apie padėtį ir sprendimų dėl bendro diplomatinio reagavimo priėmimas,*** 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

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***;***	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***, kuriomis taip pat remiamas reagavimo į solidarumo sąlygos taikymą koordinavimas politiniu lygmeniu***. Komisija šiuo tikslu turėtų naudoti aukšto lygmens tarpsektorinį krizės koordinavimo procesą ARGUS. Jei krizė susijusi su svarbiais išorės arba BSGP aspektais, turėtų būti panaudotas Europos išorės veiksmų tarnybos (EIVT) reagavimo į krizę mechanizmas***, taip pat visos priemonės, kuriomis siekiama apsaugoti BSGP misijas bei operacijas ir Sąjungos delegacijas. Be to, Sąjunga turėtų visapusiškai naudotis savo kibernetinio saugumo diplomatijos priemonių rinkiniu;***

Pakeitimas 11

Pasiūlymas dėl direktyvos
40 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(40a) valstybės narės turėtų apsvarstyti galimybę aktyvią kibernetinės gynybos programą įtraukti į jų nacionalinę kibernetinio saugumo strategiją, kuri apima reguliarias bendras valstybių narių ir tarptautinių organizacijų mokymo pratybas. Tokia programa turėtų užtikrinti sinchronizuotą galimybę realiu laiku aptikti, nustatyti, išanalizuoti ir sušvelninti grėsmes. Aktyvi kibernetinė gynyba veikia tinklo greičiu, naudodama jutiklius, programinę įrangą ir žvalgybos

	informaciją, kad idealiu atveju aptiktų ir sustabdytų piktavališką veiklą, kol ji dar nepaveikė tinklų ir sistemų. Be to, valstybės narės turėtų gerokai patobulinti dalijimosi informacija metodą, kad nustatytų bendrą ryšių standartą, kuris galėtų būti naudojamas įslaptintai ir neįslaptintai informacijai, siekiant sustiprinti greitus veiksmus. Sąjunga ir valstybės narės taip pat turėtų stiprinti savo gebėjimus nustatyti kibernetinių išpuolių autorius, kad būtų galima veiksmingai ir proporcingai bei laikantis tarptautinės teisės normų atgrasyti nuo kibernetinių išpuolių ir į juos reaguoti;

Pakeitimas 12

Pasiūlymas dėl direktyvos
40 b konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(40b) valstybės narės savo nacionalinėse kibernetinio saugumo strategijose turėtų pateikti aktyvią kibernetinės gynybos programą. Aktyvi kibernetinė gynyba yra iniciatyvus tinklo saugumo pažeidimų nustatymas, analizė ir šalinimas tikruoju laiku naudojant pajėgumus, esančius už nukentėjusio tinklo ribų. Ji grindžiama gynybos strategija, pagal kurią neįtraukiamos į priešininkų kritiškai svarbią civilinę infrastruktūrą nukreiptos puolamosios priemonės, kurios pažeistų tarptautinę teisę (pvz., 1977 m. Ženevos konvencijų Papildomo protokolo nuostatas). Gebėjimas greitai ir automatiškai dalytis informacija apie grėsmes ir ją suprasti, analizė, perspėjimai apie kibernetinę veiklą ir reagavimo veiksmai yra itin svarbūs, kad būtų sudarytos sąlygos vieningomis pastangomis sėkmingai aptikti kibernetinius išpuolius ir užkirsti jiems kelią. Aktyvi kibernetinės gynybos veikla galėtų apimti e. pašto serverių konfigūracijas, interneto svetainių

	konfigūracijas, registravimo galimybes ir DNS filtravimą. Valstybė narė turėtų priimti politiką, kuria būtų užtikrinta kuo didesnė prieiga prie geriausiai veikiančių kibernetinio saugumo priemonių, remiamos įmonės, mažosios ir vidutinės įmonės ir mažų finansinių galimybių turinčios įmonės, teikiant privilegijas, dotacijas, paskolas ar mokestines lengvatas, skirtas aukščiausio lygio kibernetinio saugumo produktų ir paslaugų įsigijimui, ir vengiant, kad jų išlaidos taptų diskriminaciniu aspektu. Valstybės narės taip pat turėtų siekti skatinti partnerystes su akademinėmis įstaigomis ir kitais mokslinių tyrimų centrais, kurių tikslas – skatinti mokslinių tyrimų ir technologinės plėtros kibernetinio saugumo programą, kad taikant plataus pobūdžio požiūrį būtų plėtojamos naujos bendros technologijos, priemonės ir įgūdžiai, taikomi tiek civiliniuose, tiek gynybos sektoriuose. Partnerystės turėtų būti finansuojamos naudojant esamas ir naujas finansavimo priemones, kurias remia Komisija;

Pakeitimas 13

Pasiūlymas dėl direktyvos
43 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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;	***rizikos valdymo sistemas ir*** jų saugaus tobulinimo procedūras, kokybę ***pagal Sąjungos kibernetinio saugumo standartus***;

Pakeitimas 14

Pasiūlymas dėl direktyvos
43 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(43a) galimi netechniniai rizikos veiksniai, kaip antai nederama trečiosios šalies įtaka tiekėjams ir paslaugų teikėjams, ypač alternatyvių valdymo modelių atveju, apima paslėptas pažeidžiamas vietas arba apėjimo būdus ir galimus sisteminius tiekimo sutrikimus, ypač technologinio susaistymo arba priklausomybės nuo tiekėjų atveju. Kadangi pažeidžiamų gynybos sektoriaus elementų išnaudojimas gali sukelti didelių trikdžių ir padaryti didelės žalos, gynybos pramonės kibernetiniam saugumui reikia specialių priemonių tiekimo grandinių, visų pirma žemesnių tiekimo grandinių subjektų, kuriems nereikia prieigos prie įslaptintos informacijos, tačiau kurie galėtų kelti didelę riziką visam sektoriui, saugumui užtikrinti. Ypatingas dėmesys turėtų būti skiriamas poveikiui, kurį pažeidimas galėtų turėti, ir grėsmei manipuliuoti tinklo duomenimis, dėl ko ypatingos svarbos gynybos ištekliai gali tapti nenaudingais ar net jų operacinės sistemos nustatomos valdyti rankiniu būdu, dėl ko jos tampa neapsaugotos nuo užgrobimo;

Pakeitimas 15

Pasiūlymas dėl direktyvos
46 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*

(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;	(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***, Europos Sąjungos kibernetinio saugumo agentūra (***ENISA***) ir Europos išorės veiksmų tarnyba***, 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;
[21] 2019 m. kovo 26 d. Komisijos rekomendacija (ES) 2019/534 dėl 5G tinklų kibernetinio saugumo (OL L 88, 2019 3 29, p. 42).	[21] 2019 m. kovo 26 d. Komisijos rekomendacija (ES) 2019/534 dėl 5G tinklų kibernetinio saugumo (OL L 88, 2019 3 29, p. 42).

Pakeitimas 16

Pasiūlymas dėl direktyvos
68 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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. ***Be to, valstybės narės***

būti taikomi visapusiškai laikantis Sąjungos konkurencijos taisyklių ir Sąjungos teisės nuostatų dėl duomenų apsaugos***;***	***taip pat galėtų išnagrinėti galimybę užmegzti ryšius su panašių pažiūrų šalimis partnerėmis.*** Tie mechanizmai turėtų būti taikomi visapusiškai laikantis Sąjungos konkurencijos taisyklių ir Sąjungos teisės nuostatų dėl duomenų apsaugos***. Tuo pačiu tikslu valstybės narės turėtų remti kompetentingas institucijas ir CSIRT, kad jos sukurtų nemokamą arba prieinamą kibernetinio saugumo pagalbą, švietimą ir audito programas subjektams, kuriems ši direktyva netaikoma, visų pirma startuoliams, MVĮ ir nevyriausybinėms organizacijoms;***

Pakeitimas 17

Pasiūlymas dėl direktyvos
68 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(68a) atsižvelgiant į tai, kad kibernetinis saugumas apima tiek civilinį, tiek ir karinį aspektą, taip pat turėtų būti skatinamas keitimasis informacija tarp sektorių (gynybos, civilinės, teisėsaugos ir išorės veiksmų). Jungtinis kibernetinis padalinys galėtų atlikti svarbų vaidmenį apsaugant Sąjungą nuo kibernetinių išpuolių, padėdamas subjektams pasiekti bendrą supratimą apie grėsmių aplinką ir koordinuojant savo atsaką;

Pakeitimas 18

Pasiūlymas dėl direktyvos
73 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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,	(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;	koks būtų tinkamas baudos dydis, priežiūros institucija turėtų atsižvelgti į bendrą pajamų lygį valstybėje narėje ir į ekonominę to asmens padėtį***, nepažeidžiant šios direktyvos tikslų***. 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;

Pakeitimas 19

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) politiką dėl kibernetinio saugumo klausimų IRT produktų ir paslaugų, kuriuos esminiai ir svarbūs subjektai naudoja teikdami savo paslaugas, tiekimo grandinėje;	a) politiką dėl kibernetinio saugumo klausimų IRT produktų ir paslaugų, kuriuos esminiai ir svarbūs subjektai naudoja teikdami savo paslaugas, tiekimo grandinėje***, remiantis išsamiu galimų grėsmių tiekimo grandinėms vertinimu***;

Pakeitimas 20

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies b a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ba) politiką, kuria skatinamas sąveikumas ir bendrų Sąjungos kibernetinio saugumo standartų laikymasis;

Pakeitimas 21

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies d punktas

Komisijos siūlomas tekstas	*Pakeitimas*
d) politiką, susijusią su bendru atvirojo interneto viešojo pagrindo prieinamumu ir vientisumu;	d) politiką, susijusią su bendru atvirojo interneto viešojo pagrindo prieinamumu ir vientisumu***, įskaitant interneto magistralių ir, kai taikoma, povandeninių ryšių kabelių kibernetinį saugumą***;

Pakeitimas 22

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies f punktas

Komisijos siūlomas tekstas	*Pakeitimas*
f) politiką dėl akademinių ir mokslinių tyrimų institucijų rėmimo ***siekiant tobulinti*** kibernetinio saugumo priemones ir saugią tinklų infrastruktūrą;	f) politiką dėl akademinių ir mokslinių tyrimų institucijų rėmimo***, joms vykdant šios srities mokslinius tyrimus bei kuriant*** kibernetinio saugumo priemones ir saugią tinklų infrastruktūrą;

Pakeitimas 23

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies h punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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***.***	h) politiką, kuria sprendžiami konkretūs ***startuolių,*** MVĮ ***ir NVO***, visų pirma į šios direktyvos taikymo sritį nepatenkančių ***startuolių,*** MVĮ ***ir NVO***, poreikiai, ir pateikiamos gairės bei parama ***jiems*** gerinant savo atsparumą kibernetinio saugumo grėsmėms***, reaguojant į kibernetinio saugumo incidentus ir siekiant gauti kibernetinio saugumo pagalbą;***

Pakeitimas 24

Pasiūlymas dėl direktyvos
5 straipsnio 2 punkto h a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ha) politika, kuria skatinamas laisvo naudojimo kodo programinės įrangos naudojimas ir kūrimas.

Pakeitimas 25

Pasiūlymas dėl direktyvos
6 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	1. Kiekviena valstybė narė paskiria vieną iš savo CSIRT, kaip nurodyta 9 straipsnyje, ***privalomo atsakingo*** pažeidžiamumų ***atskleidimo koordintore***. 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.

Pakeitimas 26

Pasiūlymas dėl direktyvos
6 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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	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.	pažeidžiamumus. ***Pagal 10 straipsnio 2 dalį CSIRT turi sudaryti palankesnes sąlygas subjektams, kurie nepatenka į šios direktyvos taikymo sritį, visų pirma startuoliams, MVĮ ir NVO, gauti informaciją apie Europos pažeidžiamumo registre užregistruotus pažeidžiamus trūkumus, kartu teikiant rizikos mažinimo pagalbą.*** 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.

Pakeitimas 27

Pasiūlymas dėl direktyvos
7 straipsnio 3 dalies f punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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***, įskaitant reagavimą į atitinkamus prašymus pagal solidarumo sąlygą***.

Pakeitimas 28

Pasiūlymas dėl direktyvos
7 straipsnio 4 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
4. Valstybės narės praneša Komisijai apie savo kompetentingų institucijų paskyrimą, nurodytą 1 dalyje, ir pateikia savo nacionalinius reagavimo į	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.	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. ***Didelio masto kibernetinio incidento ir krizės, susijusių su daugiau nei viena valstybe nare ir svarbių Sąjungos lygmeniu, atveju nustatomas tinkamas krizių valdymas ir administravimas. Tokios struktūros organizuoja keitimąsi informacija, koordinavimą ir bendradarbiavimą su Sąjungos išorės saugumo ir karinių krizių valdymo struktūromis ir valstybių narių įstaigomis, atsakingomis už saugumą ir gynybą.***

Pakeitimas 29

Pasiūlymas dėl direktyvos
9 straipsnio 4 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	4a. CSIRT bendradarbiauja ir keičiasi atitinkama informacija su nacionalinėmis institucijomis, atsakingomis už visuomenės saugumo, gynybos ir nacionalinio saugumo palaikymą.

Pakeitimas 30

Pasiūlymas dėl direktyvos
9 straipsnio 4 b dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	4b. CSIRT turi bendradarbiauti ir, nedarant poveikio Sąjungos teisei, visų pirma Reglamentui (ES) 2016/679, keistis atitinkama informacija su patikimomis trečiosiomis valstybėmis ir tarptautinėmis organizacijomis apie kibernetines grėsmes, pažeidžiamumą, geriausią patirtį

ir standartus.

Pakeitimas 31

Pasiūlymas dėl direktyvos
9 straipsnio 4 c dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	4c. CSIRT, nedarant poveikio Sąjungos teisei, visų pirma Reglamentui (ES) 2016/679, teikia kibernetinio saugumo pagalbą CSIRT arba lygiavertėms struktūroms Sąjungos šalyse kandidatėse ir kitose trečiosiose šalyse Vakarų Balkanuose ir Rytų partnerystės valstybėse.

Pakeitimas 32

Pasiūlymas dėl direktyvos
10 straipsnio 2 dalies e a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ea) sukuriant nemokamą arba prieinamą kibernetinio saugumo pagalbą, švietimą ir audito programas subjektams, kuriems ši direktyva netaikoma, visų pirma startuoliams, MVĮ ir NVO;

Pakeitimas 33

Pasiūlymas dėl direktyvos
11 straipsnio 4 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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	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***, nacionalinių dirbtinio intelekto priežiūros institucijų, nacionalinių***

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

Pakeitimas 34

Pasiūlymas dėl direktyvos
12 straipsnio 3 dalies įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	3. Bendradarbiavimo grupę sudaro valstybių narių, Komisijos***, EU-CyCLONe,*** ENISA ***ir Europos gynybos agentūros*** atstovai. Europos išorės veiksmų tarnyba Bendradarbiavimo grupėje dalyvauja stebėtojos teisėmis. ***Nacionalinės dirbtinio intelekto priežiūros institucijos, nacionalinės duomenų valdymo kompetentingos institucijos ir*** Europos priežiūros institucijos (EPI) pagal Reglamento (ES) XXXX/XXXX [DORA reglamentas] 17 straipsnio 5 dalies c punktą gali dalyvauti Bendradarbiavimo grupės veikloje.

Pakeitimas 35

Pasiūlymas dėl direktyvos
12 straipsnio 4 dalies e a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ea) nedarant poveikio Sąjungos teisei, bendradarbiauti, teikti savitarpio pagalbą

	ir keistis geriausios praktikos pavyzdžiais bei informacija su patikimomis trečiosiomis šalimis ir tarptautinėmis organizacijomis;

Pakeitimas 36

Pasiūlymas dėl direktyvos
13 straipsnio 3 dalies k punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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;	k) bendradarbiauja ir keičiasi informacija su regioniniais ir Sąjungos lygmens saugumo operacijų centrais (SOC) ***ir, kai tinkama, su kariniais CERT***, kad pagerintų bendrą informuotumą apie padėtį, susijusią su incidentais ir grėsmėmis visoje Sąjungoje;

Pakeitimas 37

Pasiūlymas dėl direktyvos
14 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	2. „EU-CyCLONe“ sudaro valstybių narių krizių valdymo institucijų, paskirtų pagal 7 straipsnį, Komisijos***, EIVT*** ir ENISA atstovai. ENISA teikia tinklo sekretoriato paslaugas ir padeda saugiai keistis informacija. ***Tokioms nacionalinėms krizių valdymo institucijoms pataria pilietine visuomene grindžiama patariamoji grupė. Didelio masto, Sąjungos lygmens kibernetinio saugumo incidentų ir krizių, susijusių su daugiau nei viena valstybe nare, atveju nustatoma Sąjungos lygmens krizių valdymo struktūra, įtraukiant visus susijusius veikėjus. Tą struktūrą sudaro Jungtinis kibernetinio saugumo padalinys, CSIRT, CSIRT tinklas, Koordinavimo grupė, Komisija, EIVT ir ENISA. Ji taip pat parengia ir įgyvendina priemones, susijusias su solidarumo***

sąlygos taikymu ir naudojimu.

Pakeitimas 38

Pasiūlymas dėl direktyvos
14 straipsnio 3 dalies a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) didina pasirengimo valdyti didelio masto incidentus ir krizes lygį;	a) didina pasirengimo valdyti didelio masto incidentus ir krizes lygį ***ir palaiko ryšius su valstybių narių agentūromis, atsakingomis už valstybės saugumą ir teritorinę gynybą***;

Pakeitimas 39

Pasiūlymas dėl direktyvos
17 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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. ***Valstybės narės turi skatinti pagrindinius ir svarbius subjektus reguliariai vertinti šio straipsnio 1 dalyje nurodytų valdymo organų narius, ar jų įgūdžiai yra pakankami siekiant užtikrinti, kad būtų laikomasi 18 straipsnio.***

Pakeitimas 40

Pasiūlymas dėl direktyvos
18 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
3. Valstybės narės užtikrina, kad, svarstydami 2 dalies d punkte nurodytas tinkamas priemones, subjektai atsižvelgtų į	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.	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 ***pagal Sąjungos kibernetinio saugumo standartus ir teisės aktus, taip pat galimus ne techninius rizikos veiksnius, kaip antai paslėptas pažeidžiamumas arba apėjimo būdai ir galimi sisteminiai tiekimo sutrikimai***.

Pakeitimas 41

Pasiūlymas dėl direktyvos
19 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	1. Bendradarbiavimo grupė, bendradarbiaudama su Komisija***,*** ENISA ***ir Europos išorės veiksmų tarnyba***, 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.

Pakeitimas 42

Pasiūlymas dėl direktyvos
19 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	2. Komisija, pasikonsultavusi su Bendradarbiavimo grupe***,*** ENISA ***ir Europos išorės veiksmų tarnyba***, nustato konkrečias ypatingos svarbos IRT paslaugas, sistemas ar produktus, dėl kurių gali būti atliekamas 1 dalyje nurodytas koordinuotas rizikos vertinimas.

Pakeitimas 43

Pasiūlymas dėl direktyvos
19 straipsnio 2a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	2a. Nustačiusi konkrečioms ypatingos svarbos IRT paslaugoms, sistemoms ar gamybos tiekimo grandinėms kylančią riziką, Komisija, pasikonsultavusi su Bendradarbiavimo grupe, ENISA ir Europos išorės veiksmų tarnyba, pateikia rekomendacijas valstybėms narėms ir šiame reglamente apibrėžtoms nacionalinėms kompetentingoms institucijoms, kaip pašalinti nustatytą riziką ir padidinti atsparumą jai.

Pakeitimas 44

Pasiūlymas dėl direktyvos
25 straipsnio 1 dalies c a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ca) informaciją apie valdymo organą, atsakingą už 18 straipsnyje apibrėžtas kibernetinio saugumo rizikos valdymo priemones, kaip apibrėžta 17 straipsnyje;

Pakeitimas 45

Pasiūlymas dėl direktyvos
29 straipsnio 2 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
c) atlikti tikslingus saugumo auditus, pagrįstus rizikos vertinimais arba prieinama informacija apie riziką;	c) atlikti tikslingus saugumo auditus, pagrįstus rizikos vertinimais arba prieinama informacija apie riziką***, įskaitant informaciją apie riziką, susijusią su tiekimo grandinėmis, kaip apibrėžta 18 straipsnio 3 dalyje***;

Pakeitimas 46

Pasiūlymas dėl direktyvos

30 straipsnio 2 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
b) atlikti tikslingus saugumo auditus, pagrįstus rizikos vertinimais arba prieinama informacija apie riziką;	b) atlikti tikslingus saugumo auditus, pagrįstus rizikos vertinimais arba prieinama informacija apie riziką***, įskaitant informaciją apie riziką, susijusią su tiekimo grandinėmis, kaip apibrėžta 18 straipsnio 3 dalyje***;

Pakeitimas 47

Pasiūlymas dėl direktyvos
I PRIEDAS – ESMINIAI SUBJEKTAI: SEKTORIAI, PASEKTORIAI IR SUBJEKTŲ RŪŠYS – Sektorius – 6 a (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	6a. Švietimas ir moksliniai tyrimai — Aukštojo mokslo institucijos ir mokslo tiriamosios įstaigos

Pakeitimas 48

Pasiūlymas dėl direktyvos
I PRIEDAS – ESMINIAI SUBJEKTAI: SEKTORIAI, PASEKTORIAI IR SUBJEKTŲ RŪŠYS – Sektorius –9. Viešasis administravimas – Subjekto rūšis

Komisijos siūlomas tekstas	*Pakeitimas*
– Centrinės valdžios viešojo administravimo subjektai	– Centrinės valdžios viešojo administravimo subjektai
– Reglamento (EB) Nr. 1059/2003([27]) I priede išvardytų NUTS 1 lygio regionų viešojo administravimo subjektai	– Reglamento (EB) Nr. 1059/2003([27, ***27a (nauja)***]) I priede išvardytų NUTS 1 lygio regionų viešojo administravimo subjektai
– Reglamento (EB) Nr. 1059/2003 I priede išvardytų NUTS 2 lygio regionų viešojo administravimo subjektai	– Reglamento (EB) Nr. 1059/2003(***[27b] (nauja)***) I priede išvardytų NUTS 2 lygio regionų viešojo administravimo subjektai
[27] 2003 m. gegužės 26 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1059/2003 dėl bendro teritorinių statistinių vienetų klasifikatoriaus (NUTS)	[27] 2003 m. gegužės 26 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1059/2003 dėl bendro teritorinių statistinių vienetų klasifikatoriaus (NUTS)

nustatymo (OL L 154, 2003 6 21, p. 1).	nustatymo (OL L 154, 2003 6 21, p. 1).
	27a (nauja) ***Arba lygiaverčiai administraciniai vienetai tose valstybėse narėse, kuriose NUTS klasifikatorius dar neatsispindi administracijos institucinėje struktūroje.***
	27b (nauja) ***Arba lygiaverčiai administraciniai vienetai tose valstybėse narėse, kuriose NUTS klasifikatorius dar neatsispindi administracijos institucinėje struktūroje.***

NUOMONĘ TEIKIANČIO KOMITETO PROCEDŪRA

Pavadinimas	Priemonės aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, Direktyvos (ES) 2016/1148 panaikinimas
Nuorodos	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Atsakingas komitetas Paskelbimo plenariniame posėdyje data	ITRE 21.1.2021
Nuomonę pateikė Paskelbimo plenariniame posėdyje data	AFET 21.1.2021
Nuomonės referentas (-ė) Paskyrimo data	Markéta Gregorová 22.2.2021
Svarstymas komitete	25.5.2021 16.6.2021 17.6.2021
Priėmimo data	14.7.2021
Galutinio balsavimo rezultatai	+: 59 –: 5 0: 6
Posėdyje per galutinį balsavimą dalyvavę nariai	Alviina Alametsä, Alexander Alexandrov Yordanov, Maria Arena, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Reinhard Bütikofer, Fabio Massimo Castaldo, Susanna Ceccardi, Włodzimierz Cimoszewicz, Katalin Cseh, Tanja Fajon, Anna Fotyga, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Raphaël Glucksmann, Klemen Grošelj, Bernard Guetta, Márton Gyöngyösi, Andrzej Halicki, Sandra Kalniete, Dietmar Köster, Maximilian Krah, Andrius Kubilius, Ilhan Kyuchyuk, David Lega, Miriam Lexmann, Nathalie Loiseau, Antonio López-Istúriz White, Jaak Madison, Claudiu Manda, Thierry Mariani, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Javier Nart, Urmas Paet, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Manu Pineda, Giuliano Pisapia, Thijs Reuten, Jérôme Rivière, María Soraya Rodríguez Ramos, Nacho Sánchez Amor, Isabel Santos, Jacek Saryusz-Wolski, Andreas Schieder, Radosław Sikorski, Jordi Solé, Sergei Stanishev, Tineke Strik, Hermann Tertsch, Hilde Vautmans, Harald Vilimsky, Idoia Villanueva Ruiz, Viola Von Cramon-Taubadel, Thomas Waitz, Witold Jan Waszczykowski, Charlie Weimers, Isabel Wiseler-Lima, Salima Yenbou, Željana Zovko
Posėdyje per galutinį balsavimą dalyvavę pavaduojantys nariai	Ioan-Rareş Bogdan, Andrey Kovatchev, Marisa Matias, Gabriel Mato, Milan Zver

GALUTINIS VARDINIS BALSAVIMAS NUOMONĘ TEIKIANČIAME KOMITETE

59	+
ECR	Anna Fotyga, Jacek Saryusz-Wolski, Hermann Tertsch, Witold Jan Waszczykowski
ID	Anna Bonfrisco, Susanna Ceccardi
NI	Fabio Massimo Castaldo, Márton Gyöngyösi
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Ioan-Rareş Bogdan, Michael Gahler, Sunčana Glavak, Andrzej Halicki, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Miriam Lexmann, Antonio López-Istúriz White, Gabriel Mato, Vangelis Meimarakis, Francisco José Millán Mon, Radosław Sikorski, Isabel Wiseler-Lima, Željana Zovko, Milan Zver
RENEW	Petras Auštrevičius, Katalin Cseh, Klemen Grošelj, Bernard Guetta, Ilhan Kyuchyuk, Nathalie Loiseau, Javier Nart, Urmas Paet, María Soraya Rodríguez Ramos, Hilde Vautmans
S&D	Maria Arena, Włodzimierz Cimoszewicz, Tanja Fajon, Raphaël Glucksmann, Dietmar Köster, Claudiu Manda, Sven Mikser, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Isabel Santos, Andreas Schieder, Sergei Stanishev
Verts/ALE	Alviina Alametsä, Reinhard Bütikofer, Jordi Solé, Tineke Strik, Viola Von Cramon-Taubadel, Thomas Waitz, Salima Yenbou

5	-
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Marisa Matias, Manu Pineda, Idoia Villanueva Ruiz

6	0
ECR	Charlie Weimers
ID	Maximilian Krah, Jaak Madison, Thierry Mariani, Jérôme Rivière, Harald Vilimsky

Sutartiniai ženklai:
+ : už
- : prieš
0 : susilaikė

14.7.2021

VIDAUS RINKOS IR VARTOTOJŲ APSAUGOS KOMITETO NUOMONĖ

pateikta Pramonės, mokslinių tyrimų ir energetikos komitetui

dėl pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Nuomonės referentas: Morten Løkkegaard

TRUMPAS PAGRINDIMAS

Apskritai nuomonės referentas palankiai vertina pasiūlymą dėl teisėkūros procedūra priimamos direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti (TIS 2). Nuomonės referentas mano, kad vis labiau skaitmenizuotame pasaulyje saugumas internete yra būtinas siekiant užtikrinti saugią skaitmeninę aplinką ir bendrosios rinkos veikimą, kur vartotojai ir ekonominės veiklos vykdytojai galėtų veikti laisvai.

Pasiūlymas dėl TIS 2 direktyvos yra svarbus patobulinimas, palyginti su Direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (TIS 1). Jame išvardijami pagrindiniai TIS 1 trūkumai, kaip antai žemas įmonių ir sektorių kibernetinio atsparumo lygis, nevienodas atsparumas ir žemas bendro informuotumo apie padėtį lygis, taip pat bendro reagavimo į krizę nebuvimas valstybėse narėse ir tarp jų. Nuomonės referentas palankiai vertina siekį ištaisyti šiuos trūkumus TIS 2 direktyvoje.

Taikymo sritis

Nuomonės referentas džiaugiasi, kad buvo išplėsta pasiūlymo dėl TIS 2 direktyvos taikymo sritis, visų pirma įtraukiant naujus sektorius, pvz., viešojo administravimo. Pateiktas išsamus sektorių ir paslaugų sąrašas neabejotinai sumažins valstybių narių veiksmų laisvę nustatant konkrečius subjektus, kuriems taikoma ši direktyva, ir taip bus sumažintas bendrosios rinkos susiskaidymas.

Sektoriams ir paslaugoms, kuriems taikoma ši direktyva, Komisija siūlo dydžio ribos taisyklę, kaip vienodą kriterijų, pagal kurį nustatomi subjektai, patenkantys į šios direktyvos taikymo sritį. Šis kriterijus neabejotinai yra privalumas, nes juo užtikrinamas teisinis tikrumas ir mažinami skirtumai tarp valstybių narių.

Nepaisant to, kad nuomonės referentas palankiai vertina išplėstą sektoriais grindžiamą taikymo sritį, jis vis dėlto mano, kad šis bendras kriterijus turėtų būti derinamas su kiekvieno sektoriaus subjektų svarbos įvertinimu. Tai leistų į direktyvos taikymo sritį neįtraukti vidutinių ir didelių subjektų, kurie, atlikus rizikos vertinimą, laikomi nedidelės svarbos ir mažai priklausomi nuo kitų ypatingos svarbos subjektų.

Nuomonės referentas pabrėžia, kad tai neturėtų būti laikoma atverta galimybe skirtingai interpretacijai tarp valstybių narių. Siekiant užtikrinti, kad taip nebūtų paskatintas nenuoseklus įgyvendinimas valstybėse narėse, Komisija raginama pateikti aiškias gaires šiuo klausimu.

Galiausiai, nors nuomonės referentas teigiamai vertina, kad į taikymo sritį neįtrauktos labai mažos ir mažosios įmonės, jis vis dėlto mano, kad reikia skatinti jų savanorišką įsitraukimą, nes labai maži ir mažieji subjektai taip pat patiria kibernetinius išpuolius ir jų neigiamą poveikį.

Koordinuotos kibernetinio saugumo reguliavimo sistemos

Nuomonės referentas teigiamai vertina skyrių, kuriame apibrėžiami įvairūs nacionalinių kibernetinio saugumo strategijų elementai ir jų krizių valdymo priemonės. Pagal savo nacionalinę kibernetinio saugumo strategiją valstybėms narėms siūloma priimti politiką, kuria būtų skatinama naudoti kriptografiją ir šifravimą, ypač MVĮ.

Nuomonės referentas palankiai vertina ENISA kuriamą Europos pažeidžiamumų registrą, tačiau mano, jog svarbu, kad registruojant būtų paisoma verslo konfidencialumo ir komercinių paslapčių ir subjektams nebūtų be reikalo užkraunama našta.

Valstybių narių bendradarbiavimas

Ypač teigiamai vertinamas sistemingesnis valstybių narių bendradarbiavimas Bendradarbiavimo grupėje, CSIRT tinkle ir TIS 2 direktyva naujai sukurtoje už didelio masto incidentus atsakingoje grupėje. Tačiau reikia užtikrinti, kad būtų didinamas valstybių narių tarpusavio pasitikėjimas ir noras keistis informacija, nes šis veiksmingas bendradarbiavimas yra labai svarbus užtikrinant aukštą kibernetinio saugumo lygį ES.

Atsižvelgiant į šią poziciją buvo parengta keletas pakeitimų siekiant sustiprinti tinklų vaidmenį. Visų pirma nuomonės referentas mano, kad tarpusavio vertinimai yra produktyvus būdas padidinti bendrą valstybių narių pasitikėjimą, ir pritaria tam, kad jie turėtų atlikti esminį vaidmenį vertinant atskirų valstybių narių kibernetinio saugumo politikos veiksmingumą.

Kibernetinio saugumo rizikos valdymas

Rizikos vertinimo išplėtimas įtraukiant visą tiekimo grandinę (18 ir 19 straipsniai) yra vertinamas teigiamai, tačiau nuomonės referentas pabrėžia, kad šis punktas turi būti patikslintas, kad būtų pateiktos aiškios gairės subjektams, kuriems taikomas šis reikalavimas, ir valstybėms narėms, kai jos atlieka koordinuotą ypatingos svarbos sektorių ar tiekimo grandinių saugumo rizikos vertinimą.

Pareigos pranešti

Nuomonės referentas mano, kad reikėtų geriau išaiškinti keletą konkrečių peržiūrėtos direktyvos punktų, visų pirma susijusių su kai kuriais įpareigojimais, taikomais įmonėms pagal

TIS 2 direktyvą. Nuomonės referentas siekia, kad būtų sumažinta biurokratija ir sudarytos palankesnės sąlygos įmonėms laikytis naujų taisyklių, atsižvelgiant į galutinį tikslą – veiksmingai įgyvendinti direktyvą.

Nuomonės referento pasiūlymas yra pratęsti siūlomą pareigos pranešti terminą pradiniams pranešimams nuo 24 valandų iki 72 valandų, kad įmonės galėtų veiksmingai reaguoti į vykdomą kibernetinį išpuolį prieš teikiant pranešimą. Be to, siūloma išbraukti nuorodą į privalomą pranešimą apie vadinamuosius „galimus incidentus“.

PAKEITIMAI

Vidaus rinkos ir vartotojų apsaugos komitetas ragina atsakingą Pramonės, mokslinių tyrimų ir energetikos komitetą atsižvelgti į šiuos pakeitimus:

Pakeitimas 1

Pasiūlymas dėl direktyvos
5 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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 ***ir stiprinti vidaus rinką***, 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;

Pakeitimas 2
Pasiūlymas dėl direktyvos
6a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(6a) Direktyva nedaromas poveikis taisyklėms, nustatytoms Sąjungos teisės aktuose dėl asmens duomenų apsaugos;

Pakeitimas 3
Pasiūlymas dėl direktyvos
9 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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; ***Komisija turėtų pateikti aiškias gaires dėl kriterijų, pagal kuriuos būtų nustatoma, kurie mažieji arba labai maži subjektai yra esminiai arba svarbūs, ypač kai teikia paslaugas keliose valstybėse narėse;***

Pakeitimas 4
Pasiūlymas dėl direktyvos
10 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(10) Komisija, bendradarbiaudama su Bendradarbiavimo grupe, ***gali*** paskelbti labai mažoms ir mažosioms įmonėms taikomų kriterijų įgyvendinimo gaires;	(10) Komisija, bendradarbiaudama su Bendradarbiavimo grupe, ***turėtų*** paskelbti labai mažoms ir mažosioms įmonėms taikomų kriterijų įgyvendinimo gaires;

Pakeitimas 5
Pasiūlymas dėl direktyvos
12 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(12a) Išplėtus šios direktyvos taikymo sritį, reikia įtraukti subjektus, kuriems taikomas konkretiems sektoriams skirtas reguliavimas. Kad būtų išvengta reglamentavimo dubliavimosi ar naštos, Komisija turėtų užtikrinti, kad konkretiems sektoriams skirti teisės aktai, pagal kuriuos reikalaujama, kad esminiai ar svarbūs subjektai priimtų kibernetinio saugumo rizikos valdymo priemones arba praneštų apie incidentus ar dideles kibernetines grėsmes, atitiktų šią direktyvą;

Pakeitimas 6
Pasiūlymas dėl direktyvos
12 b konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(12b) Komisija turėtų kartu su šia direktyva paskelbti aiškias gaires, kad padėtų užtikrinti įgyvendinimo suderinimą visose valstybėse narėse ir būtų išvengta susiskaidymo;

Pakeitimas 7
Pasiūlymas dėl direktyvos
12 c konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(12c) Komisija taip pat turėtų parengti gaires, skirtas padėti valstybėms narėms tinkamai įgyvendinti nuostatas dėl taikymo srities ir įvertinti šioje direktyvoje nustatytų įpareigojimų proporcingumą, atsižvelgiant į subjektų, kuriems taikoma ši direktyva, svarbą, ypač kai jos taikomos subjektams, kurių verslo modeliai arba

veiklos aplinka yra sudėtingi, kai subjektas vienu metu gali atitikti ir esminiams, ir svarbiems subjektams nustatytus kriterijus arba tuo pat metu vykdyti veiklą, kurios dalis patenka į šios direktyvos taikymo sritį, o dalis nepatenka. Tais atvejais, kai subjektų pagrindinė veikla nepatenka į šios direktyvos taikymo sritį, o kai kuri kita nepagrindinė veikla patenka į jos taikymo sritį, direktyvos nuostatos turėtų būti taikomos tik subjekto funkcijai ar padalinio lygmeniui, kuris patenka į šios direktyvos taikymo sritį;

Pakeitimas 8
Pasiūlymas dėl direktyvos
14 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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 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	(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 ***nacionalinėse*** kibernetinio saugumo strategijose būtų numatyta politikos sistema, kurioje būtų tvirčiau koordinuojama pagal šią direktyvą kompetentingos institucijos ir pagal Direktyvą (ES) XXX/XXX kompetentingos institucijos veikla ***pranešant apie incidentus,*** dalijantis informacija apie ***incidentus, vos neįvykusius*** 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,

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;

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;

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

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

Pakeitimas 9
Pasiūlymas dėl direktyvos
15 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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***, vidaus rinka*** 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, ***patikimų*** domenų vardų serverius ir rekursinius keitiklius***, taip pat privatumo arba įgaliotojo serverio domenų vardų registravimo paslaugų teikėjams, domenų brokeriams ar perpardavėjams ir visoms kitoms paslaugoms, susijusioms su domenų vardų registravimu***;

Pakeitimas 10
Pasiūlymas dėl direktyvos
20 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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 ***ir kad reikia saugoti vidaus rinką įgyvendinant bendras strategijas ir veiksmus Sąjungos lygmeniu***;

Pakeitimas 11
Pasiūlymas dėl direktyvos
23 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(23) kompetentingos institucijos arba	(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;	CSIRT turėtų ***standartizuotai,*** 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. 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;

Pakeitimas 12
Pasiūlymas dėl direktyvos
25 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(25) ***Siekiant nustatyti, sumažinti ar užkardyti specifines grėsmes, 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;
[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	[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).	panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1).

Pakeitimas 13
Pasiūlymas dėl direktyvos
26 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(26a) Įgyvendindamos savo nacionalines kibernetinio saugumo strategijas valstybės narės turėtų priimti pažangių sistemų skatinimo ir integravimo į kibernetinio saugumo incidentų ir grėsmių prevencijos ir nustatymo politiką. Siekdamos apsaugoti vartotojus, valstybės narės, vadovaudamosi savo nacionalinėmis kibernetinio saugumo strategijomis, turėtų įgyvendinti informuotumo apie kibernetinį saugumą ir raštingumo didinimo politiką. Priimdamos nacionalines kibernetinio saugumo strategijas, valstybės narės turėtų sukurti politikos sistemas, skirtas teisėtos prieigos prie informacijos klausimams spręsti;

Pakeitimas 14
Pasiūlymas dėl direktyvos
27 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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,	(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 ***ir kuris dėl to kelia pavojų vidaus rinkai***. Priklausomai nuo jų priežasties ir poveikio, didelio masto incidentai gali stiprėti ir virsti plataus masto krizėmis, dėl kurių vidaus rinka

kad tokie incidentai yra labai įvairaus masto ir dažniausiai tarpvalstybinio pobūdžio, valstybės narės ir atitinkamos ES institucijos, įstaigos ir agentūros turėtų bendradarbiauti techniniu, operatyviniu ir politiniu lygmenimis, kad tinkamai koordinuotų atsaką visoje Sąjungoje;

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

---

[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).

[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).

Pakeitimas 15
Pasiūlymas dėl direktyvos
28 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(28) kadangi tinklų ir informacinių sistemų pažeidžiamumų išnaudojimas gali sukelti rimtus sutrikimus ir žalą ***įmonėms ir vartotojams***, 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

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;	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;

Pakeitimas 16
Pasiūlymas dėl direktyvos
28 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(28a) Komisija, ENISA ir valstybės narės turėtų tęsti tarptautinį derinimą su rizikos valdymo standartais ir dabartine pramonės sektoriaus gerąją patirtimi rizikos valdymo srityje, pavyzdžiui, tiekimo grandinės saugumo vertinimų, dalijimosi informacija ir pažeidžiamumų atskleidimo srityse;

Pakeitimas 17
Pasiūlymas dėl direktyvos
30 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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 ***duomenų bazę***, ***kurioje*** 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;	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;

Pakeitimas 18
Pasiūlymas dėl direktyvos
31 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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***;	(31) nors panašūs pažeidžiamumų registrai arba duomenų bazės jau yra sukurti, jų prieglobą vykdo ir juos tvarko subjektai, kurie nėra įsisteigę Sąjungoje. ENISA ***tvarkoma*** pažeidžiamumų ***duomenų bazė*** padėtų užtikrinti didesnį paskelbimo proceso iki oficialaus pažeidžiamumų atskleidimo skaidrumą ir atsparumą panašių paslaugų teikimo sutrikimo arba nutraukimo atvejais. Siekdama išvengti ***pastangų*** dubliavimo ir ***kiek įmanoma siekti*** papildomumo, ENISA turėtų išnagrinėti galimybę sudaryti ***struktūrizuotus*** bendradarbiavimo susitarimus su ***trečiųjų valstybių jurisdikcijose esančiomis pažeidžiamumo duomenų bazėmis ar*** registrais ***ir perduoti ataskaitas atitinkamiems registrams, jei tokiais veiksmais nepažeidžiama konfidencialumo ir komercinių paslapčių apsauga***;

Pakeitimas 19
Pasiūlymas dėl direktyvos
32 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(32) Bendradarbiavimo grupė turėtų kas dvejus metus parengti darbo programą, įskaitant veiksmus, kurių grupė turi imtis, kad pasiektų savo tikslus ir įvykdytų	(32) Bendradarbiavimo grupė turėtų ***aptarti politinius prioritetus ir pagrindinius uždavinius kibernetinio saugumo srityje ir*** kas dvejus metus

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;

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;

Pakeitimas 20
Pasiūlymas dėl direktyvos
32 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(32a) Bendradarbiavimo grupę turėtų sudaryti valstybių narių, Komisijos ir ENISA atstovai;

Pakeitimas 21
Pasiūlymas dėl direktyvos
34 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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);	(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)**,**

	taip pat kitas atitinkamas Sąjungos įstaigas ir agentūras;

Pakeitimas 22
Pasiūlymas dėl direktyvos
35 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(35) kompetentingoms institucijoms ir CSIRT turėtų būti suteikti įgaliojimai dalyvauti pareigūnų iš kitų valstybių narių mainų programose ***ir bendrose mokymo programose*** siekiant pagerinti bendradarbiavimą ***ir valstybių narių tarpusavio pasitikėjimą***. Kompetentingos institucijos turėtų imtis būtinų priemonių, kad pareigūnai iš kitų valstybių narių galėtų veiksmingai dalyvauti priimančiosios kompetentingos institucijos ***arba CSIRT*** veikloje;

Pakeitimas 23
Pasiūlymas dėl direktyvos
39 konstatuojamoji dalis

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

Pakeitimas 24
Pasiūlymas dėl direktyvos
45 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(45a) be to, subjektai taip pat turėtų užtikrinti tinkamą savo darbuotojų švietimą ir mokymą visuose savo organizacijos lygmenyse;

Pakeitimas 25
Pasiūlymas dėl direktyvos
46 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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 ***kiekviename sektoriuje nustatyti***, ***kurios paslaugos*** yra ypatingos svarbos IRT paslaugos, sistemos ar produktai, atitinkamos grėsmės ir pažeidžiamumai;
[21] 2019 m. kovo 26 d. Komisijos rekomendacija (ES) 2019/534 dėl 5G tinklų kibernetinio saugumo (OL L 88, 2019 3 29, p. 42).	[21] 2019 m. kovo 26 d. Komisijos rekomendacija (ES) 2019/534 dėl 5G tinklų kibernetinio saugumo (OL L 88, 2019 3 29, p. 42).

Pakeitimas 26
Pasiūlymas dėl direktyvos
47 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(47) atliekant tiekimo grandinės rizikos vertinimus, atsižvelgiant į atitinkamo sektoriaus ypatumus ***ir svarbą***, 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;	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;

Pakeitimas 27
Pasiūlymas dėl direktyvos
51 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(51) vidaus rinka labiau nei kada nors anksčiau priklauso nuo interneto veikimo. Beveik visų pagrindinių ir svarbių subjektų paslaugos priklauso nuo internetu teikiamų paslaugų***, o vartotojai pasikliauja internetu pagrindinėse savo kasdienio gyvenimo srityse***. 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;

Pakeitimas 28
Pasiūlymas dėl direktyvos
52 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(52) ***subjektai turėtų siekti*** informuoti savo paslaugų gavėjus apie konkrečias ir dideles grėsmes ir apie priemones, kurių jie gali imtis, kad sumažintų jiems kylančią riziką***, ypač kai tokiomis priemonėmis galima geriau apsaugoti vartotojus. Tai*** 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 ***ir parengta lengvai suprantama kalba***;

Pakeitimas 29
Pasiūlymas dėl direktyvos
53 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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 ***papildomas*** priemones, kurių jie gali imtis savo ***prietaisų ir*** ryšių saugumui užtikrinti, pavyzdžiui, naudodami konkrečių rūšių programinę įrangą arba šifravimo technologijas;

Pakeitimas 30
Pasiūlymas dėl direktyvos
54 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(54) siekiant užtikrinti elektroninių ryšių tinklų ir paslaugų saugumą, turėtų būti skatinama naudoti šifravimą, visų pirma ištisinį šifravimą, ir, kai būtina, jis turėtų	(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;	būti privalomas tokių paslaugų ir tinklų teikėjams laikantis pritaikytosios duomenų apsaugos ir standartizuotosios duomenų apsaugos principų ***kibernetinio saugumo rizikos valdymo priemonių taikymo*** tikslais. Ištisinio šifravimo naudojimas ***nepažeidžia*** valstybių narių ***įgaliojimų, politikos ir procedūrų, kuriais jos užtikrina*** 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; ***Imantis bet kokių veiksmų turi būti griežtai laikomasi proporcingumo ir subsidiarumo principų;***

Pakeitimas 31
Pasiūlymas dėl direktyvos
55 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(55) šia direktyva nustatomas ***nuoseklus*** 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 ***arba vos neįvykusį incidentą***, jie turėtų pateikti pradinį pranešimą per ***72*** valandas, o ***ne vėliau kaip per tris mėnesius nuo pirminio pranešimo pateikimo pateikti išsamią ataskaitą, o*** galutinę ataskaitą **–** ne vėliau kaip per vieną mėnesį ***nuo incidento sušvelninimo***. Pradiniame pranešime turėtų

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***;

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. ***Prieš pateikiant pradinį pranešimą per pirmąsias 24 valandas turėtų būti pateiktas išankstinis įspėjimas, neįpareigojant atskleisti papildomos informacijos; Šis išankstinis įspėjimas turėtų būti pateikiamas kuo skubiau, kad subjektai galėtų greitai kreiptis pagalbos į kompetentingas institucijas arba CSIRT, o kompetentingos institucijos arba CSIRT galėtų sumažinti galimą incidento, apie kurį pranešta, plitimą, ir CSIRT galėtų pasinaudoti juo, kaip informavimo apie padėtį priemone.*** 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 ***numatytų terminų***;

Pakeitimas 32
Pasiūlymas dėl direktyvos
56 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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;	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 ***ir vadovautis vienkartinio duomenų pateikimo principu***, 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;

Pakeitimas 33
Pasiūlymas dėl direktyvos
59 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(59) siekiant užtikrinti DNS saugumą, stabilumą ir atsparumą, būtina turėti tikslias***, patikrintas*** 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;

Pakeitimas 34
Pasiūlymas dėl direktyvos
61 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(61) siekiant užtikrinti tikslių ir išsamių	(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;

domenų vardų registracijos duomenų prieinamumą, aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys ***domenų vardų registravimo paslaugas (įskaitant paslaugas, kurias teikia domenų vardų registrai ir registratoriai, privatumo arba įgaliotojo serverio*** domenų vardų registravimo ***paslaugų teikėjai, domenų brokeriai ar perpardavėjai, ir visas kitas*** paslaugas***, susijusias su domenų vardų registravimu***), 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;

Pakeitimas 35
Pasiūlymas dėl direktyvos
68 konstatuojamoji dalis

Komisijos siūlomas tekstas

(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;

Pakeitimas

(68) subjektai turėtų***,*** skatinami ***ir remiami valstybių narių,*** 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;

Pakeitimas 36
Pasiūlymas dėl direktyvos
69 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(69) subjektų, valdžios institucijų, CERT, CSIRT ir saugumo technologijų bei paslaugų teikėjų vykdomas asmens duomenų tvarkymas ***apsiribojant tuo, kas*** tikrai būtina ir proporcinga siekiant užtikrinti tinklų ir informacijos saugumą, ***užtikrinti vartotojų apsaugą,*** 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;

Pakeitimas 37
Pasiūlymas dėl direktyvos
70 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(70) siekiant sustiprinti priežiūros įgaliojimus ir veiksmus, padedančius užtikrinti veiksmingą reikalavimų laikymąsi, ***taip pat siekiant užtikrinti bendrą aukštą saugumo lygį visame skaitmeniniame sektoriuje, be kita ko, užkertant kelią naudotojams ar kitiems***

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;

tinklams, informacinėms sistemoms ir paslaugoms keliamai rizikai, 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****, atsižvelgiant į rizika grindžiamą požiūrį***. 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***, išskyrus tuos atvejus, kai nustatomas įrodomas pareigų nesilaikymas***;

Pakeitimas 38
Pasiūlymas dėl direktyvos
76 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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 esminių subjektų teikiamų ***atitinkamų*** paslaugų teikimu. 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

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;	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;

Pakeitimas 39
Pasiūlymas dėl direktyvos
79 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(79) turėtų būti nustatytas tarpusavio vertinimo mechanizmas, pagal kurį valstybių narių ***ir ENISA*** paskirti ekspertai galėtų įvertinti, kaip įgyvendinama kibernetinio saugumo politika, įskaitant valstybių narių pajėgumų lygį ir turimus išteklius***, taip pat būtų galima keistis geriausia praktika***;

Pakeitimas 40
Pasiūlymas dėl direktyvos
80 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(80) siekiant atsižvelgti į naujas	(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;	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 ***turėtų būti suteikti įgaliojimai priimti deleguotuosius aktus, kuriais nustatomi techniniai elementai, susiję su rizikos valdymo priemonėmis. Komisijai*** taip pat turėtų būti suteikti įgaliojimai priimti deleguotuosius aktus, ***kuriuose*** būtų ***nurodyta, kokios rūšies informaciją teikia esminiai ir svarbūs subjektai apie bet kokį incidentą***, ***turintį didelį poveikį jų paslaugų teikimui, arba apie visus vos neįvykusius incidentus,*** ir ***nurodomi atvejai, kuriais incidentas turėtų būti laikomas reikšmingu***. 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;
[26] OL L 123, 2016 5 12, p. 1.	[26] OL L 123, 2016 5 12, p. 1.

Pakeitimas 41
Pasiūlymas dėl direktyvos
81 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(81) siekiant užtikrinti vienodas	(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];	atitinkamų šios direktyvos nuostatų, susijusių su Bendradarbiavimo grupės veikimui būtina procedūrine tvarka, 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];
[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).	[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).

Pakeitimas 42
Pasiūlymas dėl direktyvos
1 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
1. Šia direktyva nustatomos priemonės, kuriomis siekiama užtikrinti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje.	1. Šia direktyva nustatomos priemonės, kuriomis siekiama užtikrinti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje***, kad vartotojams ir ekonominės veiklos vykdytojams būtų sukurta patikima skaitmeninė aplinka ir būtų pagerintas vidaus rinkos veikimas ir pašalintos kliūtys jam***.

Pakeitimas 43
Pasiūlymas dėl direktyvos
2 straipsnio 2 dalies 1 pastraipos įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. Tačiau, nepaisant subjektų dydžio, ši direktyva taikoma I ir II prieduose ***nurodytiems*** subjektams, kai:	2. Tačiau, nepaisant subjektų dydžio, ši direktyva taikoma I ir II prieduose ***nurodytos rūšies*** subjektams, kai:

Pakeitimas 44
Pasiūlymas dėl direktyvos
2 straipsnio 2 dalies 2 a pastraipa (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	Komisija parengia gaires, kad padėtų valstybėms narėms tinkamai įgyvendinti nuostatas dėl taikymo srities ir kad konkretiems svarbiems subjektams būtų leidžiama nukrypti nuo direktyvos arba kai kurių jos nuostatų taikymo srities, atsižvelgiant į jų žemą svarbos lygį jų konkrečiame sektoriuje ir (arba) nedidelę jų priklausomybę nuo kitų sektorių ar paslaugų rūšių. Valstybės narės, visapusiškai atsižvelgdamos į Komisijos gaires, praneša Komisijai apie savo motyvuotus sprendimus šiuo klausimu.

Pakeitimas 45
Pasiūlymas dėl direktyvos
4 straipsnio 1 dalies 4 punktas

Komisijos siūlomas tekstas	*Pakeitimas*
4) nacionalinė kibernetinio saugumo strategija – nuosekli valstybės narės sistema, kurioje nustatyti tos valstybės narės tinklų ir informacinių sistemų saugumo strateginiai tikslai ir prioritetai;	4) nacionalinė kibernetinio saugumo strategija – nuosekli valstybės narės sistema, kurioje nustatyti tos valstybės narės tinklų ir informacinių sistemų saugumo strateginiai tikslai ir prioritetai ***bei politikos priemonės, kurios yra būtinos jiems pasiekti***;

Pakeitimas 46
Pasiūlymas dėl direktyvos
4 straipsnio 1 dalies 5 a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	5a) tarpvalstybinis incidentas – incidentas, darantis poveikį operatoriams, kuriuos prižiūri bent dviejų skirtingų valstybių narių nacionalinės

kompetentingos institucijos;

Pakeitimas 47
Pasiūlymas dėl direktyvos
4 straipsnio 1 dalies 6 a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	6a) vos neįvykęs incidentas – įvykis, kuris galėjo sukelti potencialią žalą, tačiau faktiniam jo atsitikimui buvo sėkmingai užkirstas kelias;

Pakeitimas 48
Pasiūlymas dėl direktyvos
4 straipsnio 1 dalies 15 a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	15a) domenų vardų registravimo paslaugos – paslaugos, kurias teikia domenų vardų registrai ir registratoriai, privatumo arba įgaliotojo serverio domenų vardų registravimo paslaugų teikėjai, domenų brokeriai ar perpardavėjai, ir visos kitos paslaugos, susijusios su domenų vardų registravimu;

Pakeitimas 49
Pasiūlymas dėl direktyvos
5 straipsnio 1 dalies įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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:	1. Kiekviena valstybė narė priima nacionalinę kibernetinio saugumo strategiją, kurioje apibrėžiami strateginiai tikslai ir tinkamos politikos bei reguliavimo priemonės, ***įskaitant tinkamus žmogiškuosius ir finansinius išteklius,*** kad būtų pasiektas ir išlaikytas aukšto lygmens kibernetinis saugumas. Nacionalinėje kibernetinio saugumo strategijoje visų pirma pateikiama:

Pakeitimas 50
Pasiūlymas dėl direktyvos
5 straipsnio 1 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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;	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***, įskaitant tuos subjektus, kurie atsakingi už kibernetinę žvalgybą ir kibernetinę gynybą***;

Pakeitimas 51
Pasiūlymas dėl direktyvos
5 straipsnio 1 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
c) vertinimas, atliktas siekiant nustatyti atitinkamus objektus ir kibernetinio saugumo riziką toje valstybėje narėje***;***	c) vertinimas, atliktas siekiant nustatyti atitinkamus objektus ir kibernetinio saugumo riziką toje valstybėje narėje***, įskaitant galimą stygių, kuris gali turėti neigiamos įtakos bendrai rinkai.***

Pakeitimas 52
Pasiūlymas dėl direktyvos
5 straipsnio 1 dalies e punktas

Komisijos siūlomas tekstas	*Pakeitimas*
e) įvairių institucijų ir dalyvių, dalyvaujančių įgyvendinant nacionalinę kibernetinio saugumo strategiją, sąrašas;	e) įvairių institucijų ir dalyvių, dalyvaujančių įgyvendinant nacionalinę kibernetinio saugumo strategiją, ***įskaitant MVĮ skirtą vieno langelio sistemą,*** sąrašas;

Pakeitimas 53
Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
b) gaires dėl su kibernetiniu saugumu	b) gaires dėl su kibernetiniu saugumu

susijusių reikalavimų, taikomų IRT produktams ir paslaugoms viešuosiuose pirkimuose, ir tokių reikalavimų specifikacijų;	susijusių reikalavimų, taikomų IRT produktams ir paslaugoms viešuosiuose pirkimuose, ir tokių reikalavimų specifikacijų***, įskaitant atvirųjų kibernetinio saugumo produktų naudojimą***;

Pakeitimas 54
Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
c) suderinto pažeidžiamumų atskleidimo, kaip apibrėžta 6 straipsnyje, skatinimo ir palengvinimo politiką;	c) suderinto pažeidžiamumų atskleidimo, kaip apibrėžta 6 straipsnyje, skatinimo ir palengvinimo politiką***, įskaitant gaires ir gerąją patirtį, pagrįstą jau nustatytais tarptautiniu mastu pripažįstamais pažeidžiamumo valdymo ir atskleidimo standartais***;

Pakeitimas 55
Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies e punktas

Komisijos siūlomas tekstas	*Pakeitimas*
e) politiką ***dėl*** kibernetinio saugumo ***įgūdžių skatinimo***, ***informuotumo didinimo ir*** mokslinių tyrimų ir technologinės plėtros ***iniciatyvų***;	e) politiką***, kuria skatinamas vartotojų kibernetinis saugumas, didinamas jų informuotumas apie kibernetines grėsmes, didinamas kibernetinis raštingumas, didinamas naudotojų pasitikėjimas, technologiškai neutralūs*** kibernetinio saugumo ***įgūdžiai ir švietimas***, ***taip pat skatinamos*** mokslinių tyrimų ir technologinės plėtros ***iniciatyvos ir susietųjų produktų kibernetinis saugumas***;

Pakeitimas 56
Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies e a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ea) politiką dėl kriptografijos ir šifravimo naudojimo skatinimo, visų pirma MVĮ;

Pakeitimas 57
Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies h punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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.	h) politiką, kuria ***skatinamas kibernetinis saugumas ir*** sprendžiami konkretūs MVĮ ***poreikiai***, ***susiję su šioje direktyvoje nustatytų pareigų vykdymu, taip pat specifiniai*** į šios direktyvos taikymo sritį nepatenkančių MVĮ poreikiai, ir pateikiamos gairės bei parama joms gerinant savo atsparumą kibernetinio saugumo grėsmėms***, įskaitant, pavyzdžiui, finansavimą ir švietimą, kuriais siekiama padėti įgyvendinti kibernetinio saugumo priemones***.

Pakeitimas 58
Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies h a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ha) ši politika apima nacionalinio bendrojo MVĮ informacinio centro steigimą ir efektyviausio skaitmeninių inovacijų centrų ir turimų lėšų naudojimo siekiant atitinkamų politikos tikslų sistemos nustatymą;

Pakeitimas 59
Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies h b punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	hb) politika, kuria skatinamas nuoseklus ir sinergiškas turimų lėšų naudojimas;

Pakeitimas 60
Pasiūlymas dėl direktyvos
5 straipsnio 4 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
4. Valstybės narės, remdamosi pagrindiniais veiklos rezultatų rodikliais, vertina savo nacionalines kibernetinio saugumo strategijas ne rečiau kaip kas ketverius metus ir 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.	4. Valstybės narės, remdamosi pagrindiniais veiklos rezultatų rodikliais, vertina savo nacionalines kibernetinio saugumo strategijas ne rečiau kaip kas ketverius metus ir 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. ***ENISA taip pat teikia rekomendacijas valstybėms narėms dėl pagrindinių veiklos rezultatų rodiklių, skirtų nacionalinei strategijai vertinti, kuriuos būtų galima palygti Sąjungos lygmeniu, rengimo.***

Pakeitimas 61
Pasiūlymas dėl direktyvos
6 straipsnio pavadinimas

Komisijos siūlomas tekstas	*Pakeitimas*
Suderintas pažeidžiamumų atskleidimas ir Europos pažeidžiamumų ***registras***	Suderintas pažeidžiamumų atskleidimas ir Europos pažeidžiamumų ***duomenų bazė***

Pakeitimas 62
Pasiūlymas dėl direktyvos
6 straipsnio 2 punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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.	2. ENISA sukuria ir tvarko Europos pažeidžiamumų ***duomenų bazę***. Tuo tikslu ENISA sukuria ir prižiūri tinkamas informacines sistemas, politiką ir procedūras, ***taip pat tinkamą informacijos atskleidimo politiką,*** visų pirma siekdama sudaryti sąlygas svarbiems ir esminiams subjektams bei jų tinklų ir informacinių sistemų tiekėjams atskleisti ir ***lengvai*** registruoti IRT produktų ar paslaugų pažeidžiamumus, taip pat visoms suinteresuotosioms šalims suteikti prieigą prie ***atitinkamos*** registre pateiktos informacijos apie pažeidžiamumus***, jeigu tokie veiksmai nekenkia konfidencialumo ir komercinių paslapčių apsaugai***. ***Pažeidžiamumų duomenų bazėje*** 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. ***Siekdama išvengti veiksmų dubliavimo, ENISA sudaro dalijimosi informacija susitarimą ir struktūrinio bendradarbiavimo susitarimą su Bendro pažeidžiamumo ir rizikos (CVE) registru ir, kai tinkama, su kitomis duomenų bazėmis, kurias pasauliniu mastu kuria ir prižiūri patikimi partneriai.***

Pakeitimas 63
Pasiūlymas dėl direktyvos
7 straipsnio 1 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	1a. Jeigu valstybė narė paskiria daugiau kaip vieną 1 dalyje nurodytą kompetentingą instituciją, ji aiškiai

	nurodo, kuri iš šių kompetentingų institucijų atliks pagrindinio informacinio centro funkcijas įvykus didelio masto incidentui ar prasidėjus krizei.

Pakeitimas 64
Pasiūlymas dėl direktyvos
7 straipsnio 3 dalies f punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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.

Pakeitimas 65
Pasiūlymas dėl direktyvos
10 straipsnio 2 dalies d punktas

Komisijos siūlomas tekstas	*Pakeitimas*
d) užtikrina operatyvią rizikos bei incidentų analizę ir informuotumą apie kibernetinio saugumo padėtį;	d) užtikrina operatyvią rizikos bei incidentų analizę ir informuotumą apie kibernetinio saugumo padėtį***, be kita ko, analizuodama išankstinius įspėjimus ir pranešimus, kaip nurodyta 20 straipsnyje***;

Pakeitimas 66
Pasiūlymas dėl direktyvos
10 straipsnio 2 dalies e punktas

Komisijos siūlomas tekstas	*Pakeitimas*
e) subjekto prašymu ***aktyviai*** patikrina tinklų ir informacines sistemas, kurias subjektas naudoja teikdamas paslaugas;	e) subjekto prašymu patikrina tinklų ir informacines sistemas, kurias subjektas naudoja teikdamas paslaugas***, siekiant nustatyti, sumažinti ar užkardyti specifines grėsmes***;

Pakeitimas 67
Pasiūlymas dėl direktyvos
10 straipsnio 2 dalies f punktas

Komisijos siūlomas tekstas	*Pakeitimas*
f) ***dalyvauja*** CSIRT tinkle ir teikia savitarpio pagalbą kitiems tinklo nariams jų prašymu.	f) ***aktyviai dalyvauja*** CSIRT tinkle ir teikia savitarpio pagalbą kitiems tinklo nariams jų prašymu.

Pakeitimas 68
Pasiūlymas dėl direktyvos
10 straipsnio 2 dalies f a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	fa) teikia operatyvinę pagalbą ir konsultacijas I ir II prieduose nurodytiems subjektams, ypač MVĮ;

Pakeitimas 69
Pasiūlymas dėl direktyvos
10 straipsnio 2 dalies f b punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	fb) dalyvauja bendrose kibernetinio saugumo pratybose Sąjungos lygmeniu;

Pakeitimas 70
Pasiūlymas dėl direktyvos
11 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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	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 ***veiksmingai*** vykdyti, suteikiama ***tinkama*** prieiga prie duomenų

pranešė esminiai ar svarbūs subjektai pagal 20 straipsnį.	apie incidentus, apie kuriuos pranešė esminiai ar svarbūs subjektai pagal 20 straipsnį.

Pakeitimas 71
Pasiūlymas dėl direktyvos
11 straipsnio 4 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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***, taip pat bendradarbiavimą su kibernetinės gynybos ir kibernetinės žvalgybos institucijomis***.
[39] [įrašyti visą pavadinimą ir OL paskelbimo nuorodą, kai ji bus žinoma]	[39] [įrašyti visą pavadinimą ir OL paskelbimo nuorodą, kai ji bus žinoma]

Pakeitimas 72
Pasiūlymas dėl direktyvos
12 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. Bendradarbiavimo grupė vykdo savo užduotis remdamasi dvimetėmis darbo programomis, nurodytomis 6 dalyje.	2. Bendradarbiavimo grupė ***reguliariai susitinka ir*** vykdo savo užduotis remdamasi dvimetėmis darbo programomis, nurodytomis 6 dalyje.

Pakeitimas 73
Pasiūlymas dėl direktyvos
12 straipsnio 3 dalies 2 pastraipa

Komisijos siūlomas tekstas	*Pakeitimas*
Prireikus Bendradarbiavimo grupė gali pakviesti atitinkamų suinteresuotųjų šalių atstovus dalyvauti jos darbe.	Prireikus Bendradarbiavimo grupė gali pakviesti atitinkamų ***Sąjungos įstaigų ir agentūrų bei*** suinteresuotųjų šalių atstovus dalyvauti jos darbe.

Pakeitimas 74
Pasiūlymas dėl direktyvos
12 straipsnio 4 dalies a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) teikia kompetentingoms institucijoms gaires dėl šios direktyvos perkėlimo į nacionalinę teisę ir įgyvendinimo;	a) teikia kompetentingoms institucijoms gaires dėl šios direktyvos perkėlimo į nacionalinę teisę ir įgyvendinimo ***bei skatina vienodą jos įgyvendinimą valstybėse narėse***;

Pakeitimas 75
Pasiūlymas dėl direktyvos
12 straipsnio 4 dalies a a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	aa) keičiasi informacija apie politinius prioritetus ir pagrindinius uždavinius kibernetinio saugumo srityje ir nustato pagrindinius kibernetinio saugumo tikslus;

Pakeitimas 76
Pasiūlymas dėl direktyvos
12 straipsnio 4 dalies a b punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ab) aptaria valstybių narių nacionalines strategijas ir jų parengtį;

Pakeitimas 77
Pasiūlymas dėl direktyvos
12 straipsnio 4 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
c) keičiasi patarimais ir bendradarbiauja su Komisija dėl naujų kibernetinio saugumo politikos iniciatyvų;	c) keičiasi patarimais ir bendradarbiauja su Komisija dėl naujų kibernetinio saugumo politikos iniciatyvų***, o su Europos išorės veiksmų tarnyba – dėl geopolitinių kibernetinio saugumo Sąjungoje aspektų***;

Pakeitimas 78
Pasiūlymas dėl direktyvos
12 straipsnio 4 dalies f punktas

Komisijos siūlomas tekstas	*Pakeitimas*
f) aptaria 16 straipsnio 7 dalyje nurodytas tarpusavio vertinimo ataskaitas;	f) aptaria 16 straipsnio 7 dalyje nurodytas tarpusavio vertinimo ataskaitas***, įvertindama savo funkcijas ir rengdama išvadas***;

Pakeitimas 79
Pasiūlymas dėl direktyvos
12 straipsnio 4 dalies k a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ka) padeda ENISA Sąjungos lygmeniu organizuoti bendrus mokymus nacionalinėms kompetentingoms institucijoms.

Pakeitimas 80
Pasiūlymas dėl direktyvos
12 straipsnio 6 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
6. Iki… □***24*** mėnesiai po šios direktyvos įsigaliojimo dienos□, o vėliau kas dvejus metus Bendradarbiavimo grupė parengia darbo programą, skirtą	6. Iki… □***12*** 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.	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.

Pakeitimas 81
Pasiūlymas dėl direktyvos
12 straipsnio 8 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	8a. Bendradarbiavimo grupė reguliariai skelbia apibendrintą savo veiklos ataskaitą, nedarydama poveikio informacijos, kuria dalijamasi jos posėdžiuose, konfidencialumui.

Pakeitimas 82
Pasiūlymas dėl direktyvos
13 straipsnio 3 punkto a papunktis

Komisijos siūlomas tekstas	*Pakeitimas*
a) keičiasi informacija apie CSIRT pajėgumus;	a) keičiasi informacija apie CSIRT pajėgumus ***ir parengtį***;

Pakeitimas 83
Pasiūlymas dėl direktyvos
13 straipsnio 3 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
b) keičiasi svarbia informacija apie incidentus, vos neįvykusius incidentus, kibernetines grėsmes, riziką ir pažeidžiamumus;	b) keičiasi svarbia informacija apie incidentus, vos neįvykusius incidentus, kibernetines grėsmes, riziką ir pažeidžiamumus ***ir remia valstybių narių operatyvinius pajėgumus***;

Pakeitimas 84
Pasiūlymas dėl direktyvos
13 straipsnio 3 dalies d a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	da) keičiasi informacija apie tarpvalstybinius incidentus ir ją aptaria;

Pakeitimas 85
Pasiūlymas dėl direktyvos
13 straipsnio 3 dalies g punkto i a papunktis (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ia) informacijos mainais;

Pakeitimas 86
Pasiūlymas dėl direktyvos
13 straipsnio 3 dalies j punktas

Komisijos siūlomas tekstas	*Pakeitimas*
j) ***atskiros CSIRT prašymu aptaria tos*** CSIRT pajėgumus ir parengtį;	j) ***aptaria*** CSIRT pajėgumus ir parengtį;

Pakeitimas 87
Pasiūlymas dėl direktyvos
13 straipsnio 4 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	4. Atsižvelgiant į 35 straipsnyje nurodytą peržiūrą, ne vėliau kaip iki [24 mėnesiai nuo šios direktyvos įsigaliojimo datos ir paskui ***kasmet*** 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.

Pakeitimas 88
Pasiūlymas dėl direktyvos
14 straipsnio 3 dalies a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) didina pasirengimo valdyti didelio masto incidentus ir krizes lygį;	a) didina pasirengimo valdyti didelio masto incidentus ir krizes***, įskaitant tarpvalstybinio pobūdžio kibernetines grėsmes,*** lygį;

Pakeitimas 89
Pasiūlymas dėl direktyvos
14 straipsnio 5 dalis

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

Pakeitimas 90
Pasiūlymas dėl direktyvos
14 straipsnio 6 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
6. „EU-CyCLONe“ su CSIRT tinklu bendradarbiauja remdamasis sutartomis procedūrinėmis taisyklėmis.	6. „EU-CyCLONe“ su CSIRT tinklu ***glaudžiai*** bendradarbiauja remdamasis sutartomis procedūrinėmis taisyklėmis.

Pakeitimas 91
Pasiūlymas dėl direktyvos
15 straipsnio 1 dalies įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
1. ENISA, bendradarbiaudama su Komisija, kas dvejus metus rengia kibernetinio saugumo Sąjungoje būklės ataskaitą. Ataskaitoje visų pirma įvertinami šie aspektai:	1. ENISA, bendradarbiaudama su Komisija, kas dvejus metus rengia kibernetinio saugumo Sąjungoje būklės ataskaitą ***ir pateikia ją Europos Parlamentui***. Ataskaitoje visų pirma

įvertinami šie aspektai:

Pakeitimas 92
Pasiūlymas dėl direktyvos
15 straipsnio 1 dalies a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) kibernetinio saugumo pajėgumų Sąjungoje plėtojimas;	a) kibernetinio saugumo pajėgumų Sąjungoje plėtojimas***, įskaitant bendrą įgūdžių ir žinių lygį kibernetinio saugumo srityje, bendras vidaus rinkos atsparumo kibernetinėms grėsmėms lygis ir direktyvos įgyvendinimo valstybėse narėse lygis***;

Pakeitimas 93
Pasiūlymas dėl direktyvos
15 straipsnio 1 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
c) kibernetinio saugumo indeksas, kuriame atsispindi apibendrintas kibernetinio saugumo pajėgumų brandos vertinimas.	c) kibernetinio saugumo indeksas, kuriame atsispindi apibendrintas kibernetinio saugumo pajėgumų brandos vertinimas***, įskaitant bendro kibernetinio saugumo vartotojams vertinimą***.

Pakeitimas 94
Pasiūlymas dėl direktyvos
15 straipsnio 1 dalies c a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ca) geopolitiniai aspektai, turintys tiesioginį ar netiesioginį poveikį kibernetinio saugumo padėčiai Sąjungoje.

Pakeitimas 95
Pasiūlymas dėl direktyvos
16 straipsnio 1 dalies įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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:	1. Komisija, pasikonsultavusi su Bendradarbiavimo grupe ir ENISA, ir ne vėliau kaip per ***12*** 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 ***bent*** iš ***dviejų*** valstybių narių ***ir iš ENISA***, kuriose peržiūra neatlikta, ir jos apima bent šiuos aspektus:

Pakeitimas 96
Pasiūlymas dėl direktyvos
16 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	2. Metodika apima objektyvius, nediskriminacinius, ***technologiškai neutralius,*** 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.

Pakeitimas 97
Pasiūlymas dėl direktyvos
18 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
1. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai imtųsi ***tinkamų ir proporcingų*** techninių ir	1. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai imtųsi techninių ir organizacinių priemonių,

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.	siekdami valdyti tinklų ir informacinių sistemų, kurias tie subjektai naudoja teikdami savo paslaugas, saugumui kylančią riziką. ***Tos priemonės yra tinkamos ir proporcingos atsižvelgiant į sektoriaus ar paslaugų rūšies svarbą ir subjekto priklausomybės nuo kitų sektorių ar paslaugų rūšių lygį ir jos priimamos atlikus rizika grindžiamą vertinimą.*** Remiantis naujausiais technikos laimėjimais, tomis priemonėmis turi būti užtikrinamas toks tinklų ir informacinių sistemų saugumo lygis, kuris atitinka kylančią riziką. ***Visų pirma imamasi priemonių, kad būtų išvengta saugumo incidentų poveikio jų paslaugų vartotojams ir jis būtų kuo mažesnis.***

Pakeitimas 98
Pasiūlymas dėl direktyvos
18 straipsnio 2 dalies d punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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;	d) tiekimo grandinės ***saugumo rizikos vertinimo priemones***, įskaitant ***apimančias*** 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;

Pakeitimas 99
Pasiūlymas dėl direktyvos
18 straipsnio 2 dalies f punktas

Komisijos siūlomas tekstas	*Pakeitimas*
f) politiką ir procedūras (bandymai ir auditas), skirtas kibernetinio saugumo rizikos valdymo priemonių veiksmingumui įvertinti;	f) politiką ir procedūras (bandymai ir auditas) ***ir nuolatines kibernetinio saugumo pratybas***, skirtas kibernetinio saugumo rizikos valdymo priemonių veiksmingumui įvertinti;

Pakeitimas 100
Pasiūlymas dėl direktyvos
18 straipsnio 2 dalies g punktas

Komisijos siūlomas tekstas	*Pakeitimas*
g) kriptografijos ir šifravimo naudojimą**.**	g) kriptografijos***, šifravimo*** ir ***visų pirma ištisinio*** šifravimo naudojimą***;***

Pakeitimas 101
Pasiūlymas dėl direktyvos
18 straipsnio 2 dalies g a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ga) politiką, kuria siekiama užtikrinti tinkamą mokymą ir informuotumą apie kibernetinį saugumą.

Pakeitimas 102
Pasiūlymas dėl direktyvos
18 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	3. Valstybės narės užtikrina, kad, svarstydami 2 dalies d punkte nurodytas tinkamas priemones, subjektai***, kai jie turi prieigą prie atitinkamos informacijos,*** 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.

Pakeitimas 103
Pasiūlymas dėl direktyvos
18 straipsnio 5 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
5. ***Komisija gali*** priimti ***įgyvendinimo*** aktus, kuriais nustatomos 2 dalyje nurodytų aspektų techninės ir metodinės specifikacijos***. Rengdama tuos aktus***	5. ***Komisijai suteikiami įgaliojimai*** priimti ***deleguotuosius*** aktus, kuriais nustatomos 2 dalyje nurodytų aspektų techninės ir metodinės specifikacijos ir,

Komisija laikosi 37 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros ir, kiek įmanoma, ***laikosi*** tarptautinių ir Europos standartų bei atitinkamų techninių specifikacijų.

kiek įmanoma, ***laikomasi*** tarptautinių ir Europos standartų bei atitinkamų techninių specifikacijų. ***Rengdama deleguotuosius aktus, Komisija taip pat konsultuojasi su atitinkamais suinteresuotaisiais subjektais.***

Pakeitimas 104
Pasiūlymas dėl direktyvos
18 straipsnio 6 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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***.	6. ***Komisija, bendradarbiaudama su Bendradarbiavimo grupe ir ENISA***, ***teikia gaires ir geriausios praktikos pavyzdžius dėl to***, ***kaip subjektams proporcingai laikytis 2 dalyje nustatytų reikalavimų ir visų pirma tos dalies d punkte nustatyto reikalavimo***.

Pakeitimas 105
Pasiūlymas dėl direktyvos
19 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	1. ***Siekiant padidinti bendrą kibernetinio saugumo lygį, 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***, pavyzdžiui, geopolitinę riziką***.

Pakeitimas 106
Pasiūlymas dėl direktyvos
20 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
1. Valstybės narės užtikrina, kad	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.	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 ***arba bet kokiems vos neįvykusiems incidentams***. 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 ar vos neįvykusio*** incidento poveikį.

Pakeitimas 107
Pasiūlymas dėl direktyvos
20 straipsnio 1a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	1a. Siekdamos supaprastinti pareigas pranešti, valstybės narės sukuria 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.

Pakeitimas 108
Pasiūlymas dėl direktyvos
20 straipsnio 1 b dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	1b. ENISA, bendradarbiaudama su Bendradarbiavimo grupe, parengia bendrus pranešimo šablonus, pateikdama gaires, kuriomis būtų supaprastinta ir racionalizuota pagal Sąjungos teisę reikalaujama pranešimų teikimo informacija ir sumažinta bendrovėms tenkanti atitikties našta.

Pakeitimas 109
Pasiūlymas dėl direktyvos
20 straipsnio 2 dalies 1 pastraipa

Komisijos siūlomas tekstas	*Pakeitimas*
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.***	***Išbraukta.***

Pakeitimas 110
Pasiūlymas dėl direktyvos
20 straipsnio 2 dalies 2 pastraipa

Komisijos siūlomas tekstas	*Pakeitimas*
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.	***Išbraukta.***

Pakeitimas 111
Pasiūlymas dėl direktyvos
20 straipsnio 3 dalies a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) dėl incidento atitinkamas subjektas patyrė ***arba gali patirti*** didelių veiklos sutrikimų arba finansinių nuostolių;	a) dėl incidento atitinkamas subjektas patyrė didelių veiklos sutrikimų arba finansinių nuostolių;

Pakeitimas 112
Pasiūlymas dėl direktyvos
20 straipsnio 3 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
b) incidentas paveikė ***arba gali paveikti*** kitus fizinius ar juridinius asmenis dėl didelių materialinių arba neturtinių nuostolių.	b) incidentas paveikė kitus fizinius ar juridinius asmenis dėl didelių materialinių arba neturtinių nuostolių.

Pakeitimas 113
Pasiūlymas dėl direktyvos
20 straipsnio 3 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	3a. Komisijai pagal 36 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, kuriais ši direktyva papildoma nustatant pagal šio straipsnio 1 dalį pateiktinos informacijos tipą ir patikslinant atvejus, kuriais incidentas laikomas dideliu, kaip nurodyta šio straipsnio 3 dalyje.

Pakeitimas 114
Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies -a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	-a) išankstinį įspėjimą per 24 valandas po to, kai sužinoma apie incidentą, atitinkamam subjektui netaikant jokių įpareigojimų atskleisti su incidentu susijusią papildomą informaciją;

Pakeitimas 115
Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) nepagrįstai nedelsiant ir bet kuriuo atveju per ***24*** valandas nuo to laiko, kai sužinoma apie incidentą, – pradinį pranešimą, kuriame, kai taikoma,	a) nepagrįstai nedelsiant ir bet kuriuo atveju per ***72*** valandas nuo to laiko, kai sužinoma apie incidentą, – pradinį pranešimą, kuriame, kai taikoma,

nurodoma, ar incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai;	nurodoma, ar incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai;

Pakeitimas 116
Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies c punkto įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
c) ne vėliau kaip per ***vieną mėnesį*** nuo a punkte nurodytos ataskaitos pateikimo – ***galutinę*** ataskaitą, kurioje pateikiama bent ši informacija:	c) ne vėliau kaip per ***tris mėnesius*** nuo a punkte nurodytos ataskaitos pateikimo – ***išsamią*** ataskaitą, kurioje pateikiama bent ši informacija:

Pakeitimas 117
Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies c punkto i papunktis

Komisijos siūlomas tekstas	*Pakeitimas*
i) ***išsamus*** incidento, jo sunkumo ir poveikio aprašymas;	i) ***išsamesnis*** incidento, jo sunkumo ir poveikio aprašymas;

Pakeitimas 118
Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies c a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ca) jei teikiant išsamią ataskaitą pagal c punktą incidentas tebevyksta, galutinė ataskaita pateikiama praėjus mėnesiui po incidento sušvelninimo;

Pakeitimas 119
Pasiūlymas dėl direktyvos
20 straipsnio 7 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
7. Kai visuomenės informuotumas yra būtinas siekiant užkirsti kelią incidentui ar reaguoti į besitęsiantį incidentą arba kai incidento atskleidimas kitais atvejais	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.	atitinka viešąjį interesą, kompetentinga institucija arba CSIRT ir atitinkamais atvejais kitų atitinkamų valstybių narių institucijos arba CSIRT, pasikonsultavusios su atitinkamu subjektu, ***informuoja*** visuomenę apie incidentą arba pareikalauti, kad tai padarytų subjektas.

Pakeitimas 120
Pasiūlymas dėl direktyvos
20 straipsnio 8 dalis

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

Pakeitimas 121
Pasiūlymas dėl direktyvos
20 straipsnio 9 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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 ***dalį*** ir pagal 27 straipsnį. Siekdama prisidėti prie palyginamos informacijos teikimo ENISA gali paskelbti technines gaires dėl į suvestinę ataskaitą įtrauktos informacijos parametrų.

Pakeitimas 122
Pasiūlymas dėl direktyvos
20 straipsnio 10 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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].	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 ***dalį*** pranešė esminiai subjektai, nustatyti kaip ypatingos svarbos subjektai arba ypatingos svarbos subjektams lygiaverčiai subjektai, pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva].

Pakeitimas 123
Pasiūlymas dėl direktyvos
20 straipsnio 11 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	11. Komisija gali priimti įgyvendinimo aktus, kuriais išsamiau nustatoma pagal 1 ***dalį*** 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.

Pakeitimas 124
Pasiūlymas dėl direktyvos
21 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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***	1. Siekdamos įrodyti atitiktį tam tikriems 18 straipsnio reikalavimams ***ir didinti kibernetinio saugumo lygį***, valstybės narės***, pasikonsultavusios su Bendradarbiavimo grupe ir ENISA***, ***skatina esminius*** ir ***svarbius subjektus sertifikuoti*** tam tikrus IRT produktus,

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***.	paslaugas ir procesus***, kuriuos kuria esminis arba svarbus subjektas arba kurie perkami iš trečiųjų šalių, pagal*** Europos kibernetinio saugumo schemas, priimtas pagal Reglamento (ES) 2019/881 49 straipsnį, ***arba pagal panašias tarptautiniu mastu pripažintas sertifikavimo schemas. Kai įmanoma, valstybės narės skatina suderintai naudoti patvirtintas sertifikavimo sistemas***.

Pakeitimas 125
Pasiūlymas dėl direktyvos
21 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.***	2. ***Komisija reguliariai vertina priimtų Europos kibernetinio saugumo sertifikavimo schemų efektyvumą ir naudojimą pagal Reglamento (ES) 2019/881 49 straipsnį ir nustato***, kokių kategorijų ***esminius subjektus*** reikia ***skatinti*** gauti sertifikatą ir pagal kurias konkrečias Europos kibernetinio saugumo sertifikavimo schemas pagal 1 dalį.

Pakeitimas 126
Pasiūlymas dėl direktyvos
22 straipsnio -1 dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	-1. Komisija, bendradarbiaudama su ENISA, remia ir skatina standartų, kuriuos nustatė atitinkamos Sąjungos ir tarptautinės standartizacijos institucijos siekdamos vienodai įgyvendinti 18 straipsnio 1 ir 2 dalis, rengimą ir įgyvendinimą. Komisija remia standartų atnaujinimą atsižvelgiant į technologijų plėtrą.

Pakeitimas 127
Pasiūlymas dėl direktyvos
22 straipsnio 1 punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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.	1. Siekdamos skatinti vienodą 18 straipsnio 1 ir 2 dalių įgyvendinimą, valstybės narės, nereikalaudamos taikyti kokios nors konkrečios rūšies technologijos ir nesuteikdamos jai pirmenybės ***ir vadovaudamosi ENISA ir Bendradarbiavimo grupės pateiktomis gairėmis***, skatina naudotis europiniais ar tarptautiniu mastu pripažintais standartais ir specifikacijomis, kurie yra svarbūs tinklų ir informacinių sistemų saugumui.

Pakeitimas 128
Pasiūlymas dėl direktyvos
23 straipsnio pavadinimas

Komisijos siūlomas tekstas	*Pakeitimas*
Domenų vardų ir registracijos duomenų ***bazės***	Domenų vardų ir registracijos duomenų ***bazių infrastruktūra***

Pakeitimas 129
Pasiūlymas dėl direktyvos
23 straipsnio 1 punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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***, tikrintų*** 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.

Pakeitimas 130
Pasiūlymas dėl direktyvos
23 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	2. Valstybės narės užtikrina, kad 1 dalyje ***nurodytoje*** domenų vardų registracijos duomenų ***bazių infrastruktūroje*** būtų atitinkama informacija, ***įskaitant bent jau registruotojų pavadinimus, jų faktinius ir e. pašto adresus bei telefono numerius, būtinus, kad*** būtų galima nustatyti domenų vardų turėtojus ir kontaktinius centrus, administruojančius aukščiausio lygio domenų vardais pažymėtus domenų vardus***, įskaitant bent jau registruotojų pavadinimus, jų faktinius ir e. pašto adresus bei telefono numerius***, ir su jais susisiekti.

Pakeitimas 131
Pasiūlymas dėl direktyvos
23 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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 ***bazės infrastruktūroje*** būtų pateikiama tiksli***, patikrinta*** ir išsami informacija ***ir kad registruotojas nedelsdamas pakoreguotų arba ištrintų netikslius arba neišsamius duomenis***. Valstybės narės užtikrina, kad tokia politika ir procedūros būtų skelbiamos viešai.

Pakeitimas 132
Pasiūlymas dėl direktyvos
23 straipsnio 4 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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***.	4. Valstybės narės užtikrina, kad aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys domenų vardų registravimo paslaugas***, nepagrįstai nedelsdami ir bet kuriuo atveju per 24 valandas*** po domeno vardo užregistravimo ***viešai*** paskelbtų ***visus juridinių asmenų kaip registruotojų domeno registracijos duomenis***.

Pakeitimas 133
Pasiūlymas dėl direktyvos
23 straipsnio 5 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	5. Valstybės narės užtikrina, kad aukščiausio lygio domenų vardų registrai ir subjektai, teikiantys domenų vardų registravimo paslaugas, gavę tinkamai pagrįstus siekiančių gauti prieigą subjektų prašymus, ***privalėtų suteikti*** 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***, nepagrįstai nedelsdami ir bet kuriuo atveju per 72 valandas*** atsakytų į visus ***teisėtus ir tinkamai pagrįstus*** prašymus suteikti prieigą. Valstybės narės užtikrina, kad tokių duomenų atskleidimo politika ir procedūros būtų skelbiamos viešai.

Pakeitimas 134
Pasiūlymas dėl direktyvos
24 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. Taikant šią direktyvą laikoma, kad 1 dalyje nurodytų subjektų pagrindinė	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.	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. ***Tai daroma taip, kad būtų užtikrinama, kad nacionalinėms reguliavimo institucijoms netektų neproporcingai didelė našta.***

Pakeitimas 135
Pasiūlymas dėl direktyvos
25 straipsnio 1 dalies įžanginė dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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:	1. ENISA sukuria ir tvarko 24 straipsnio 1 dalyje nurodytų esminių ir svarbių subjektų registrą. ***Tuo tikslu*** subjektai ne vėliau kaip [12 mėnesių po direktyvos įsigaliojimo] pateikia ENISA šią informaciją:

Pakeitimas 136
Pasiūlymas dėl direktyvos
26 straipsnio 1 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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 ***ir prevencijos*** metodus, švelninimo strategijas arba reagavimo ir atsigavimo etapus.

Pakeitimas 137
Pasiūlymas dėl direktyvos
26 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	3. Valstybės narės nustato ***gaires***, kuriose aprašoma 2 dalyje nurodytų dalijimosi informacija susitarimų procedūra, veiklos elementai (įskaitant specialių IRT platformų naudojimą), turinys ir sąlygos. Tokiose ***gairėse*** taip pat ***pateikiama*** išsami informacija apie***, kai tinkama,*** valdžios institucijų ***ir nepriklausomų ekspertų*** 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.

Pakeitimas 138
Pasiūlymas dėl direktyvos
26 straipsnio 5 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
5. Laikydamasi Sąjungos teisės ENISA remia 2 dalyje nurodytų dalijimosi kibernetinio saugumo informacija susitarimų sudarymą, teikdama geriausios praktikos pavyzdžius ir gaires.	5. Laikydamasi Sąjungos teisės ENISA remia 2 dalyje nurodytų dalijimosi kibernetinio saugumo informacija susitarimų sudarymą, teikdama geriausios praktikos pavyzdžius ir gaires***, sudarydama sąlygas dalytis informacija Sąjungos lygmeniu ir tuo pat metu apsaugodama neskelbtiną informaciją. Esminių ir svarbių subjektų prašymu Bendradarbiavimo grupė kviečiama pateikti geriausios praktikos pavyzdžius ir gaires.***

Pakeitimas 139
Pasiūlymas dėl direktyvos
27 straipsnio -1 dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	-1. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai galėtų

	savanoriškai teikti pranešimus apie kibernetines grėsmes, kurias tie subjektai nustatė ir dėl kurių galėtų įvykti didelis incidentas. Valstybės narės užtikrina, kad šių pranešimų teikimo tikslais subjektai imtųsi veiksmų 20 straipsnyje nustatyta tvarka. Dėl savanoriškų pranešimų pranešančiajam subjektui nenustatoma jokių papildomų įpareigojimų.

Pakeitimas 140
Pasiūlymas dėl direktyvos
27 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	***1. 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 ***teikia*** 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***, bet valstybė narė jam gali skirti CSIRT pagalbą***.

Pakeitimas 141
Pasiūlymas dėl direktyvos
28 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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***, ir kad joms būtų suteiktos atitinkamos priemonės jų vaidmeniui atlikti***.

Pakeitimas 142
Pasiūlymas dėl direktyvos
28 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. Kompetentingos institucijos, nagrinėdamos incidentus, dėl kurių pažeidžiamas asmens duomenų saugumas, glaudžiai bendradarbiauja su duomenų apsaugos institucijomis.	2. Kompetentingos institucijos, nagrinėdamos incidentus, dėl kurių pažeidžiamas asmens duomenų saugumas, glaudžiai bendradarbiauja su duomenų apsaugos institucijomis***, įskaitant, jei reikia, kitų valstybių narių duomenų apsaugos institucijas***.

Pakeitimas 143
Pasiūlymas dėl direktyvos
29 straipsnio 2 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
c) ***atlikti tikslingus*** saugumo auditus, pagrįstus rizikos vertinimais arba prieinama informacija apie riziką;	c) ***tikslingus*** saugumo auditus, pagrįstus rizikos vertinimais arba prieinama informacija apie riziką***, kuriuos atlieka kvalifikuota nepriklausoma įstaiga arba kompetentinga institucija***;

Pakeitimas 144
Pasiūlymas dėl direktyvos
29 straipsnio 2 dalies f punktas

Komisijos siūlomas tekstas	*Pakeitimas*
f) prašyti leisti susipažinti su duomenimis, dokumentais ar ***bet kokia*** informacija, reikalinga jų priežiūros užduotims atlikti;	f) prašyti leisti susipažinti su ***atitinkamais*** duomenimis, dokumentais ar informacija, reikalinga jų priežiūros užduotims atlikti;

Pakeitimas 145
Pasiūlymas dėl direktyvos
29 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
3. Naudodamosi savo įgaliojimais pagal 2 dalies e–g punktus, kompetentingos institucijos nurodo prašymo tikslą ir ***prašomą*** informaciją.	3. Naudodamosi savo įgaliojimais pagal 2 dalies e–g punktus, kompetentingos institucijos nurodo prašymo tikslą ***, prašomą informaciją*** ir ***prašo pateikti tik su incidentu arba susirūpinimą keliančiu klausimu susijusią*** informaciją.

Pakeitimas 146
Pasiūlymas dėl direktyvos
29 straipsnio 5 dalies 1 pastraipos a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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;	a) sustabdyti arba prašyti, kad sertifikavimo arba leidimus išduodanti įstaiga sustabdytų sertifikavimą arba įgaliojimą, susijusį su ***atitinkamomis*** esminės įstaigos teikiamomis paslaugomis ar veikla;

Pakeitimas 147
Pasiūlymas dėl direktyvos
29 straipsnio 5 dalies 1 pastraipos b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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.	***Išbraukta.***

Pakeitimas 148
Pasiūlymas dėl direktyvos
30 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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 ***ir atsižvelgiant į rizika grindžiamą požiūrį*** imtųsi veiksmų taikydamos ex post priežiūros priemones.

Pakeitimas 149
Pasiūlymas dėl direktyvos
30 straipsnio 2 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
b) ***atlikti tikslingus*** saugumo auditus, pagrįstus rizikos vertinimais arba prieinama informacija apie riziką;	b) ***tikslingus*** saugumo auditus, pagrįstus rizikos vertinimais arba prieinama informacija apie riziką***, kuriuos atlieka kvalifikuota nepriklausoma įstaiga arba kompetentinga institucija***;

Pakeitimas 150
Pasiūlymas dėl direktyvos
30 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
3. Naudodamosi savo įgaliojimais pagal 2 dalies d arba e punktus, kompetentingos institucijos nurodo prašymo tikslą ir ***patikslina prašomą*** informaciją.	3. Naudodamosi savo įgaliojimais pagal 2 dalies d arba e punktus, kompetentingos institucijos nurodo prašymo tikslą***, prašomą informaciją*** ir ***prašo pateikti tik su incidentu arba susirūpinimą keliančiu klausimu susijusią*** informaciją.

Pakeitimas 151
Pasiūlymas dėl direktyvos
31 straipsnio 4 dalis

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

Pakeitimas 152
Pasiūlymas dėl direktyvos
32 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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 informuoja priežiūros institucijas, kompetentingas pagal to reglamento 55 ir 56 straipsnius***, nepagrįstai nedelsdamos ir bet kuriuo atveju per 72 valandas***.

Pakeitimas 153
Pasiūlymas dėl direktyvos
32 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	3. Jeigu priežiūros institucija, kompetentinga pagal Reglamentą (ES) 2016/679, yra įsteigta kitoje valstybėje narėje nei kompetentinga institucija, kompetentinga institucija ***taip pat informuoja*** toje pačioje valstybėje narėje įsteigtą priežiūros instituciją.

Pakeitimas 154
Pasiūlymas dėl direktyvos
36 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. 18 straipsnio ***6*** dalyje ir ***21*** straipsnio ***2*** dalyje nurodyti įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami penkerių metų laikotarpiui nuo […]	2. 18 straipsnio ***5*** dalyje ir ***20*** straipsnio ***3*** dalyje nurodyti įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami penkerių metų laikotarpiui nuo […]

Pakeitimas 155
Pasiūlymas dėl direktyvos
36 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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***.	3. ***Pagal 18 straipsnio 5 dalį ir 20 straipsnio 3 dalį priimtas deleguotasis aktas įsigalioja tik tuo atveju, jeigu per tris 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 trimis mėnesiais***.

Pakeitimas 156
Pasiūlymas dėl direktyvos
36 straipsnio 6 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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	6. Pagal 18 straipsnio ***5*** dalį ir ***20*** straipsnio ***3*** 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.	Parlamentas, ir Taryba praneša Komisijai, kad prieštaravimų nereikš. Europos Parlamento arba Tarybos iniciatyva šis laikotarpis pratęsiamas dviem mėnesiais.

ANNEX: LIST OF ENTITIES OR PERSONS FROM WHOM THE RAPPORTEUR HAS RECEIVED INPUT

The following list is drawn up on a purely voluntary basis under the exclusive responsibility of the rapporteur. The rapporteur has received input from the following entities or persons in the preparation of the opinion, until the adoption thereof in committee:

Person	Entity
	BSA (The Software Alliance)
	BusinessEurope
	Confederation of Danish Industries
	Danish Permanent Representation
	Deutsche Telekom
	Digital Europe
	DOT Europe
	ETNO (European Telecommunications Network Operators)
	French Permanent Representation
	German Permanent Representation
	HUAWEI
	IFPI
	INTEL
	ITI (The Information Technology Industry Council)
	Kaspersky
	MÆRSK
	Microsoft
	ICANN
	MOTION PICTURE ASSOCIATION
	Orgalim
	Palo Alto Networks

	Rettighedsalliancen

NUOMONĘ TEIKIANČIO KOMITETO PROCEDŪRA

Pavadinimas	Priemonės aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, Direktyvos (ES) 2016/1148 panaikinimas
Nuorodos	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Atsakingas komitetas Paskelbimo plenariniame posėdyje data	ITRE 21.1.2021
Nuomonę pateikė Paskelbimo plenariniame posėdyje data	IMCO 21.1.2021
Nuomonės referentas (-ė) Paskyrimo data	Morten Løkkegaard 9.2.2021
Svarstymas komitete	26.5.2021 21.6.2021
Priėmimo data	12.7.2021
Galutinio balsavimo rezultatai	+: 42 –: 1 0: 2
Posėdyje per galutinį balsavimą dalyvavę nariai	Alex Agius Saliba, Andrus Ansip, Pablo Arias Echeverría, Alessandra Basso, Brando Benifei, Adam Bielan, Hynek Blaško, Biljana Borzan, Vlad-Marius Botoş, Markus Buchheit, Andrea Caroppo, Anna Cavazzini, Dita Charanzová, Deirdre Clune, David Cormand, Carlo Fidanza, Evelyne Gebhardt, Alexandra Geese, Sandro Gozi, Maria Grapini, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Marcel Kolaja, Kateřina Konečná, Andrey Kovatchev, Jean-Lin Lacapelle, Maria-Manuel Leitão-Marques, Morten Løkkegaard, Antonius Manders, Leszek Miller, Anne-Sophie Pelletier, Miroslav Radačovský, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein, Marco Zullo
Posėdyje per galutinį balsavimą dalyvavę pavaduojantys nariai	Clara Aguilera, Maria da Graça Carvalho, Christian Doleschal, Claude Gruffat, Jiří Pospíšil, Kosma Złotowski

GALUTINIS VARDINIS BALSAVIMAS NUOMONĘ TEIKIANČIAME KOMITETE

42	+
ECR	Adam Bielan, Carlo Fidanza, Kosma Złotowski
ID	Alessandra Basso, Hynek Blaško, Markus Buchheit, Virginie Joron, Jean-Lin Lacapelle
PPE	Pablo Arias Echeverría, Andrea Caroppo, Maria da Graça Carvalho, Deirdre Clune, Christian Doleschal, Andrey Kovatchev, Antonius Manders, Jiří Pospíšil, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein
Renew	Andrus Ansip, Vlad-Marius Botoş, Dita Charanzová, Sandro Gozi, Morten Løkkegaard, Marco Zullo
S&D	Alex Agius Saliba, Clara Aguilera, Brando Benifei, Biljana Borzan, Evelyne Gebhardt, Maria Grapini, Maria-Manuel Leitão-Marques, Leszek Miller, Christel Schaldemose
The Left	Kateřina Konečná, Anne-Sophie Pelletier
Verts/ALE	Anna Cavazzini, David Cormand, Alexandra Geese, Claude Gruffat, Marcel Kolaja

1	-
NI	Miroslav Radačovský

2	0
ECR	Eugen Jurzyca
Renew	Svenja Hahn

Sutartiniai ženklai:
+ : už
- : prieš
0 : susilaikė

14.7.2021

TRANSPORTO IR TURIZMO KOMITETO NUOMONĖ

pateikta Pramonės, mokslinių tyrimų ir energetikos komitetui

dėl pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Nuomonės referentas: Jakop G. Dalunde

TRUMPAS PAGRINDIMAS

Transporto sektorius yra vis labiau pažeidžiamas ir veikiamas kibernetinio saugumo grėsmių. Dėl konkrečių sektoriaus ypatumų jis taip pat patiria įvairias kitas grėsmes. Todėl šiame nuomonės projekte pateikti pakeitimai, nors ir bendro pobūdžio, yra siūlomi turint mintyje šiuos ypatumus. Mano pasiūlymai yra svarbūs transportui dėl šių priežasčių:

- transporto veikla dažnai yra tarptautinio pobūdžio ir ją vykdant daug subjektų priklauso kelių valstybių narių jurisdikcijai. Todėl sektoriui didelį poveikį daro pernelyg dideli valstybių narių kibernetinio saugumo rizikos valdymo ir ataskaitų teikimo įpareigojimų skirtumai;

- transporto sektoriaus veikla priklauso nuo saugaus įvairių subjektų keitimosi duomenimis. Dėl logistikos subjektų tarpusavio priklausomybės nepakankamas vieno subjekto kibernetinis saugumas galėtų kelti pavojų visai sistemai ir turėti rimtų pasekmių kitų subjektų veiklai;

- Transportas yra daug darbo reikalaujantis sektorius ir todėl ypač pažeidžiamas darbuotojams kylančių kibernetinių grėsmių požiūriu.

Dėl šių priežasčių pakeitimais dėmesys sutelkiamas į šias temas: valstybių narių skirtumų, susijusių su kibernetinio saugumo įpareigojimais, lygio vertinimas, šių įpareigojimų suderinimo ne teisėkūros priemonėmis skatinimas, darbuotojų mokymo ir žinių apie kibernetinio saugumo riziką skatinimas.

Be šių bendrų aspektų, verta pažymėti, kad teikiant paslaugas transporto sektoriuje vis dažniau naudojami nuotoliniai jutikliai, kurie gali prisijungti prie interneto, o pačios transporto priemonės vis labiau skaitmeninamos. Nors šie prietaisai nebūtinai yra platesnių informacinių sistemų dalis, jiems gali reikėti atlikti specialius saugumo vertinimus.

PAKEITIMAI

Transporto ir turizmo komitetas ragina atsakingą Pramonės, mokslinių tyrimų ir energetikos komitetą atsižvelgti į šiuos pakeitimus:

Pakeitimas 1

Pasiūlymas dėl direktyvos
3 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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***;	(3) tinklų ir informacinės sistemos dėl sparčios skaitmeninės transformacijos ir visuomenės tarpusavio junglumo ***tapo pagrindiniu kasdienio gyvenimo aspektu, prisidėdamos prie naujų verslo modelių ir paslaugų, pvz., susijusių su trumpų projektų, užsakomųjų paslaugų ir platformų ekonomika, augimo***, įskaitant tarpvalstybinius mainus ***ir paslauginio judumo (MaaS) metodą***. 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 ***kenkti visuomenės gerovei,*** trukdyti vykdyti ekonominę veiklą vidaus rinkoje ***bei socialinę veiklą***, sukelti finansinių nuostolių, pakirsti naudotojų ***ir darbuotojų*** pasitikėjimą***, taip*** padaryti didelę žalą Sąjungos ekonomikai ir visuomenei ***ar net kelti terorizmo grėsmę***. Todėl kibernetinio saugumo parengtis ir veiksmingumas kaip niekad anksčiau yra labai svarbūs ***siekiant apsaugoti Sąjungos pagrindines teises ir laisves ir tinkamą*** vidaus rinkos ***veikimą. Be to, kibernetinis saugumas yra daugelio ypatingos svarbos sektorių, pavyzdžiui, transporto, bazinė didelio poveikio priemonė siekiant sėkmingai vykdyti skaitmeninę transformaciją ir visapusiškai pasinaudoti skaitmeninimo teikiama ekonomine, socialine ir tvarumo***

nauda;

Pakeitimas 2

Pasiūlymas dėl direktyvos
9 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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***. Ši veikla turėtų būti vykdoma visapusiškai suvokiant mažųjų ir vidutinių įmonių (MVĮ) specifiškumą ir ja MVĮ neturėtų būti sukurta pernelyg didelė administracinė našta;***

Pakeitimas 3

Pasiūlymas dėl direktyvos
10 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(10) Komisija, bendradarbiaudama su Bendradarbiavimo grupe, gali paskelbti labai mažoms ir mažosioms įmonėms taikomų kriterijų įgyvendinimo gaires;	(10) Komisija, bendradarbiaudama su Bendradarbiavimo grupe ***ir atitinkamomis suinteresuotosiomis šalimis***, gali paskelbti labai mažoms ir mažosioms įmonėms taikomų kriterijų įgyvendinimo gaires***. Komisija taip pat turėtų užtikrinti, kad visoms labai mažoms ir mažosioms įmonėms, kurioms taikoma ši direktyva, būtų pateiktos tinkamos rekomendacijos. Komisija, padedama valstybių narių, turėtų suteikti labai mažoms ir mažosioms įmonėms informaciją šiuo klausimu; .***

Pakeitimas 4

Pasiūlymas dėl direktyvos
12 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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. ***Siekiant išvengti teisinio netikrumo aiškinant ir taikant šią direktyvą Komisija turėtų užtikrinti šios direktyvos ir taikomų konkretiems sektoriams skirtų teisės aktų suderinamumą. Šiuo tikslu Komisija turėtų nustatyti atitinkamų teisės aktų, reglamentavimo reikalavimų ar procedūrų dubliavimąsi, kad jį pašalintų.*** 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;

Pakeitimas 5

Pasiūlymas dėl direktyvos
15 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(15a) siekiant užtikrinti, kad visa tiekimo grandinė tinkamai reaguotų į riziką ir grėsmes, reikia saugiai įgyvendinti didesnį pagrindinių ekonomikos sektorių, pvz., transporto, skaitmeninimą, kuriuo savaime būtų užtikrintas atsparumas. Todėl reikia nustatyti suderintą požiūrį, kuriuo būtų užtikrintas minimalus sujungtų prietaisų saugumo lygis, ypač tokiuose sektoriuose kaip transportas ir tais atvejais, kai jie yra įtraukti į transporto priemones ir standartiškai naudoja ištisinį šifravimą;

Pakeitimas 6

Pasiūlymas dėl direktyvos
17 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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);	(17) atsižvelgiant į novatoriškų technologijų***, pavyzdžiui, dirbtinio intelekto, naujų verslo modelių*** ir naujų ***lankstaus bei nuotolinio darbo*** modelių atsiradimą, tikimasi, kad rinkoje atsiras naujų debesijos kompiuterijos diegimo ir paslaugų modelių, atsižvelgiant į kintančius vartotojų ***ir verslo*** 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);

Pakeitimas 7

Pasiūlymas dėl direktyvos
18 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(18a) atsižvelgiant į tai, kad autonominio

	judumo diegimas atneš didelės naudos, tačiau taip pat kels įvairią naują riziką, visų pirma susijusią su eismo sauga, kibernetiniu saugumu, intelektinės nuosavybės teisėmis, duomenų apsaugos ir prieigos prie duomenų problemomis, techninė infrastruktūra, standartizavimu ir užimtumu, nepaprastai svarbu užtikrinti, kad Sąjungos teisinė sistema būtų tinkamai reaguojama į tuos iššūkius ir veiksmingai valdoma visa tinklų bei informacinių sistemų saugumui kylanti rizika;

Pakeitimas 8

Pasiūlymas dėl direktyvos
18 b konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(18b) koronaviruso pandemija parodė, kaip svarbu parengti Sąjungą skaitmeniniam dešimtmečiui ir tai, kad reikia nuolat gerinti kibernetinį atsparumą. Todėl šia direktyva siekiama nustatyti minimalias suderintos reglamentavimo sistemos veikimo taisykles, kad būtų sudarytos sąlygos skaitmeninei pertvarkai ir inovacijoms visų transporto rūšių autonominio transporto, logistikos ir eismo valdymo srityse ir sustiprintas naudotojų, visų pirma labai mažų įmonių, MVĮ bei startuolių, atsparumas kibernetiniams išpuoliams ir pajėgumas mažinti pažeidžiamumą;

Pakeitimas 9

Pasiūlymas dėl direktyvos
19 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(19) pašto paslaugų teikėjams, kaip apibrėžta Europos Parlamento ir Tarybos direktyvoje 97/67/EB[18], taip pat greitojo	(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;	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 ***arba pristatymo*** paslaugos, kai jos nėra susijusios su vienu iš šių etapų, neturėtų patekti į pašto paslaugų apibrėžtį;
[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).	[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).

Pakeitimas 10

Pasiūlymas dėl direktyvos
27 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(27a) savo nacionalinėse kibernetinio saugumo strategijose valstybės narės turėtų atsižvelgti į konkrečius MVĮ kibernetinio saugumo poreikius, t. y. nedidelį informuotumą apie kibernetinį saugumą, nuotolinio IT saugumo trūkumą, dideles kibernetinio saugumo sprendimų sąnaudas bei išaugusį grėsmės lygį. Valstybės narės turėtų turėti MVĮ skirtą kibernetinio saugumo kontaktinį centrą, kuriame būtų galima susipažinti su atitinkama informacija, naudotis paslaugomis ir gauti rekomendacijų;

Pakeitimas 11

Pasiūlymas dėl direktyvos
33 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(33) rengdama gairių dokumentus,	(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;	Bendradarbiavimo grupė turėtų nuosekliai***:*** išsiaiškinti nacionalinius sprendimus ir patirtį, įvertinti Bendradarbiavimo grupės rezultatų poveikį nacionaliniam požiūriui, aptarti įgyvendinimo problemas ir suformuluoti konkrečias rekomendacijas, ***visų pirma dėl šios direktyvos perkėlimo į nacionalinę teisę suderinimo tarp valstybių narių palengvinimo,*** į kurias turėtų būti atsižvelgiama geriau įgyvendinant dabartines taisykles. ***Bendradarbiavimo grupė taip pat turėtų išsiaiškinti nacionalinius sprendimus, kad būtų skatinamas kibernetinio saugumo sprendimų, taikomų kiekvienam konkrečiam sektoriui visoje Europoje, suderinamumas. Tai ypač svarbu tarptautinio ir tarpvalstybinio pobūdžio sektoriams, pavyzdžiui, transporto sektoriui;***

Pakeitimas 12

Pasiūlymas dėl direktyvos
34 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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);	(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 ***prireikus*** pakviesti jos veikloje dalyvauti kibernetinio saugumo politiką įgyvendinančias Sąjungos įstaigas ir agentūras, pavyzdžiui, Europos kovos su elektroniniu nusikalstamumu centrą (EC3), Europos ***kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrą, už saugų transportą atsakingas Europos Sąjungos agentūras –***

	Europos Sąjungos aviacijos saugos agentūrą (EASA)***, Europos jūrų saugumo agentūrą (EMSA), Europos Sąjungos geležinkelių agentūrą (ESGA) –*** Europos Sąjungos kosmoso programos agentūrą (EUSPA) ***ir bet kokią kitą įstaigą ir agentūrą, kurios ekspertinės žinios yra svarbios grupės diskusijoms***;

Pakeitimas 13

Pasiūlymas dėl direktyvos
37 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(37a) pernelyg dideli kibernetinio saugumo rizikos valdymo ir ataskaitų teikimo įpareigojimų skirtumai valstybėms narėms perkėlus šią direktyvą į nacionalinę teisę galėtų kelti pavojų bendram kibernetinio saugumo lygiui Sąjungoje. Todėl ENISA, bendradarbiaudama su Komisija, savo dvimetėje ataskaitoje dėl kibernetinio saugumo padėties Sąjungoje turėtų įvertinti valstybių narių kibernetinio saugumo rizikos valdymo ir ataskaitų teikimo įpareigojimų skirtumus;

Pakeitimas 14

Pasiūlymas dėl direktyvos
46 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(46a) siekiant išsaugoti ir apsaugoti ypatingos svarbos tiekimo grandines, dėmesys taip pat turėtų būti sutelktas į visos transporto ir logistikos grandinės apsaugą. Transporto ir logistikos grandinę sudaro daug tarpusavyje susijusių subjektų ir sistemų ir prekės gabenamos įvairiarūšiu būdu, naudojant oro, kelių, geležinkelių, vidaus vandenų ir jūrų transportą. Šiam procesui reikalingas greitas ir patikimas įvairių

	transporto bei logistikos grandinės grandžių keitimasis duomenimis, naudojantis įvairiomis sąsajomis. Kadangi įvairios grandinės grandys yra tarpusavyje susijusios, nepakankamas kibernetinis saugumas gali kelti grėsmę visos grandinės veikimui dėl domino efekto, kurį sukeltų kibernetinis incidentas vienoje ar keliose transporto ir logistikos grandinės dalyse;

Pakeitimas 15

Pasiūlymas dėl direktyvos
47 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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;	(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***; iva) kokiu mastu konkrečios ypatingos svarbos IRT paslaugos, sistemos ar produktai, kuriuos tiesiogiai naudoja vartotojai, yra atsparūs ir atitinka klientui palankų požiūrį,*** ir v) atsirandančių IRT paslaugų, sistemų ar

produktų atveju, jų galimą būsimą svarbą subjektų veiklai;

Pakeitimas 16

Pasiūlymas dėl direktyvos
55 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(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	(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 ***36*** 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;	nuo ***36*** valandų termino pradiniam pranešimui ir vieno mėnesio termino galutinės ataskaitos pateikimui;

Pakeitimas 17

Pasiūlymas dėl direktyvos
2 straipsnio 2 dalies 2 pastraipa

Komisijos siūlomas tekstas	*Pakeitimas*
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.	Valstybės narės***, glaudžiai bendradarbiaudamos su atitinkamomis pramonės suinteresuotosiomis šalimis,*** 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.

Pakeitimas 18

Pasiūlymas dėl direktyvos
2 straipsnio 6 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	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, ***įskaitant atitinkamų priežiūros institucijų galias, įgaliojimus ir funkcijas,*** atitinkamos šios direktyvos nuostatos, įskaitant VI skyriaus nuostatą dėl priežiūros ir vykdymo užtikrinimo, netaikomos.

Pakeitimas 19

Pasiūlymas dėl direktyvos
5 straipsnio 2 dalies h punktas

Komisijos siūlomas tekstas	*Pakeitimas*
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.	h) politiką, kuria sprendžiami konkretūs MVĮ, visų pirma į šios direktyvos taikymo sritį nepatenkančių MVĮ, poreikiai, ir pateikiamos gairės***, suteikiant reikiamą ir išsamią informaciją*** bei ***paramą*** joms gerinant savo atsparumą kibernetinio saugumo grėsmėms.

Pakeitimas 20

Pasiūlymas dėl direktyvos
12 straipsnio 4 dalies a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) teikia kompetentingoms institucijoms gaires dėl šios direktyvos perkėlimo į nacionalinę teisę ir įgyvendinimo;	a) teikia kompetentingoms institucijoms gaires dėl šios direktyvos perkėlimo į nacionalinę teisę ir įgyvendinimo***, kad būtų kuo labiau sumažinti valstybių narių kibernetinio saugumo rizikos valdymo ir ataskaitų teikimo įpareigojimų standartų skirtumai***;

Pakeitimas 21

Pasiūlymas dėl direktyvos
12 straipsnio 4 dalies b a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ba) išsiaiškina nacionalinius sprendimus, kad būtų skatinamas kibernetinio saugumo sprendimų, taikomų kiekvienam konkrečiam sektoriui visoje Sąjungoje, suderinamumas;

Pakeitimas 22

Pasiūlymas dėl direktyvos
15 straipsnio 1 dalies c a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ca) valstybių narių kibernetinio saugumo rizikos valdymo ir ataskaitų teikimo įpareigojimų skirtumai ir tai, kokiu mastu jie daro poveikį bendram kibernetinio saugumo lygiui Sąjungoje.

Pakeitimas 23

Pasiūlymas dėl direktyvos
16 straipsnio 1 dalies iii a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	iiia) rekomendacijas, kaip padidinti šios direktyvos ir taikytinų konkretiems sektoriams skirtų teisės aktų aiškinimo ir taikymo nuoseklumą bei teisinį tikrumą, daug dėmesio skiriant atitinkamų teisės aktų, reglamentavimo reikalavimų ar procedūrų dubliavimosi ir sutapimo nustatymui bei pašalinimui;

Pakeitimas 24

Pasiūlymas dėl direktyvos
18 straipsnio 2 dalies b a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ba) politiką, programas ir procedūras, kuriomis užtikrinama, kad darbuotojai turėtų pakankamai žinių, kurių reikia siekiant suprasti kibernetinio saugumo riziką, ir praktinės patirties, atitinkančios aukštus kibernetinio saugumo standartus;

Pakeitimas 25

Pasiūlymas dėl direktyvos
18 straipsnio 2 dalies e punktas

Komisijos siūlomas tekstas	*Pakeitimas*
e) tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumą,	e) tinklų ir informacinių sistemų***, įskaitant mobiliuosius elementus, pvz.,***

įskaitant pažeidžiamumo valdymą ir atskleidimą;	***transporto priemones ir nuotolinius jutiklius, jų*** įsigijimo, plėtojimo ir priežiūros saugumą, įskaitant pažeidžiamumo valdymą ir atskleidimą;

Pakeitimas 26

Pasiūlymas dėl direktyvos
18 straipsnio 5 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	5. Komisija gali priimti ***deleguotuosius*** aktus, kuriais nustatomos 2 dalyje nurodytų aspektų techninės ir metodinės specifikacijos. ***Deleguotieji aktai priimami pagal 36 straipsnį*** ir ***jais***, kiek įmanoma, ***laikomasi*** tarptautinių ir Europos standartų bei atitinkamų techninių specifikacijų.

Pakeitimas 27

Pasiūlymas dėl direktyvos
18 straipsnio 6 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	6a. Siekdama užtikrinti veiksmingą politiką ir palengvinti jos įgyvendinimą, Komisija konsultuojasi su esminiais ir svarbiais subjektais, ypač prieš priimdama 5 ir 6 dalyse nurodytus deleguotuosius aktus.

Pakeitimas 28

Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies 1 pastraipos a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) nepagrįstai nedelsiant ir bet kuriuo atveju per ***24*** valandas nuo to laiko, kai sužinoma apie incidentą, – pradinį pranešimą, kuriame, kai taikoma,	a) nepagrįstai nedelsiant ir bet kuriuo atveju per ***36*** valandas nuo to laiko, kai sužinoma apie incidentą, – pradinį pranešimą, kuriame, kai taikoma,

nurodoma, ar incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai;	nurodoma, ar incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai;

Pakeitimas 29

Pasiūlymas dėl direktyvos
20 straipsnio 4 dalies 1 pastraipos c punkto iii papunktis

Komisijos siūlomas tekstas	*Pakeitimas*
iii) taikomos ir įgyvendinamos poveikio mažinimo priemonės.	iii) taikomos ir įgyvendinamos poveikio mažinimo priemonės ***ir jų rezultatai***.

Pakeitimas 30

Pasiūlymas dėl direktyvos
20 straipsnio 11 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	11. Komisija gali priimti deleguotuosius aktus pagal 36 straipsnį, kuriais išsamiau nustatoma pagal šio straipsnio 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.

Pakeitimas 31

Pasiūlymas dėl direktyvos
21 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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	1. Siekdamos įrodyti atitiktį tam tikriems 18 straipsnio reikalavimams, valstybės narės ***skatina esminius*** ir ***svarbius subjektus sertifikuoti*** tam tikrus IRT produktus, paslaugas ir procesus***, kuriuos sukūrė esminis ar svarbus subjektas arba kurie įsigyti iš trečiųjų šalių,*** pagal konkrečias Europos

(ES) 2019/881 49 straipsnį***.*** ***Sertifikuojamus produktus***, ***paslaugas ir procesus gali kurti esminis*** arba ***svarbus subjektas arba jie gali būti perkami iš trečiųjų šalių***.

kibernetinio saugumo sertifikavimo schemas, priimtas pagal Reglamento (ES) 2019/881 49 straipsnį, arba ***pagal panašias tarptautiniu mastu pripažintas sertifikavimo schemas***.

Pakeitimas 32

Pasiūlymas dėl direktyvos
21 straipsnio 1 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	1a. Šios direktyvos reikalavimai dėl kibernetinio saugumo sertifikavimo nedaro poveikio Reglamento (ES) 2019/881 56 straipsnio 2 ir 3 dalims.

Pakeitimas 33

Pasiūlymas dėl direktyvos
21 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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.	***Išbraukta.***

Pakeitimas 34

Pasiūlymas dėl direktyvos
21 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
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***.	3. ***Siekdama padidinti bendrą kibernetinio saugumo atsparumo lygį, Komisija*** gali prašyti ENISA parengti potencialią schemą pagal Reglamento (ES) 2019/881 ***47 ir 48 straipsnius*** tais atvejais, kai nėra tinkamos Europos kibernetinio saugumo sertifikavimo ***schemos. Tokios***

potencialios schemos turi atitikti Reglamento (ES) 2019/881 56 straipsnio 2 dalyje ir 56 straipsnio 3 dalyje nustatytus reikalavimus.

NUOMONĘ TEIKIANČIO KOMITETO PROCEDŪRA

Pavadinimas	Priemonės aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, Direktyvos (ES) 2016/1148 panaikinimas
Nuorodos	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Atsakingas komitetas Paskelbimo plenariniame posėdyje data	ITRE 21.1.2021
Nuomonę pateikė Paskelbimo plenariniame posėdyje data	TRAN 21.1.2021
Nuomonės referentas (-ė) Paskyrimo data	Jakop G. Dalunde 3.2.2021
Priėmimo data	12.7.2021
Galutinio balsavimo rezultatai	+: 48 –: 0 0: 1
Posėdyje per galutinį balsavimą dalyvavę nariai	Magdalena Adamowicz, Andris Ameriks, Izaskun Bilbao Barandica, Paolo Borchia, Marco Campomenosi, Massimo Casanova, Ciarán Cuffe, Jakop G. Dalunde, Johan Danielsson, Karima Delli, Anna Deparnay-Grunenberg, Gheorghe Falcă, Giuseppe Ferrandino, Mario Furore, Søren Gade, Isabel García Muñoz, Elsi Katainen, Kateřina Konečná, Julie Lechanteux, Peter Lundgren, Benoît Lutgen, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Tilly Metz, Cláudia Monteiro de Aguiar, Caroline Nagtegaal, Jan-Christoph Oetjen, Philippe Olivier, João Pimenta Lopes, Rovana Plumb, Dominique Riquet, Dorien Rookmaker, Massimiliano Salini, Sven Schulze, Vera Tax, Barbara Thaler, Henna Virkkunen, Petar Vitanov, Elissavet Vozemberg-Vrionidi, Roberts Zīle, Kosma Złotowski
Posėdyje per galutinį balsavimą dalyvavę pavaduojantys nariai	Clare Daly, Nicola Danti, Angel Dzhambazki, Tomasz Frankowski, Michael Gahler, Maria Grapini, Alessandra Moretti, Marianne Vind

GALUTINIS VARDINIS BALSAVIMAS NUOMONĘ TEIKIANČIAME KOMITETE

48	+
ECR	Angel Dzhambazki, Peter Lundgren, Roberts Zīle, Kosma Złotowski
ID	Paolo Borchia, Marco Campomenosi, Massimo Casanova, Julie Lechanteux, Philippe Olivier
NI	Mario Furore, Dorien Rookmaker
PPE	Magdalena Adamowicz, Gheorghe Falcă, Tomasz Frankowski, Michael Gahler, Elżbieta Katarzyna Łukacijewska, Benoît Lutgen, Marian-Jean Marinescu, Cláudia Monteiro de Aguiar, Massimiliano Salini, Sven Schulze, Barbara Thaler, Henna Virkkunen, Elissavet Vozemberg-Vrionidi
RENEW	Izaskun Bilbao Barandica, Nicola Danti, Søren Gade, Elsi Katainen, Caroline Nagtegaal, Jan-Christoph Oetjen, Dominique Riquet
S&D	Andris Ameriks, Johan Danielsson, Giuseppe Ferrandino, Isabel García Muñoz, Maria Grapini, Alessandra Moretti, Rovana Plumb, Vera Tax, Marianne Vind, Petar Vitanov
The Left	Clare Daly, Kateřina Konečná
Verts/ALE	Ciarán Cuffe, Jakop G. Dalunde, Karima Delli, Anna Deparnay-Grunenberg, Tilly Metz

0	-

1	0
The Left	João Pimenta Lopes

Sutartiniai ženklai:
+ : už
- : prieš
0 : susilaikė

ATSAKINGO KOMITETO PROCEDŪRA

Pavadinimas	Priemonės aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, Direktyvos (ES) 2016/1148 panaikinimas			
Nuorodos	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)			
Pateikimo EP data	16.12.2020			
Atsakingas komitetas Paskelbimo plenariniame posėdyje data	ITRE 21.1.2021			
Nuomonę teikiantys komitetai Paskelbimo plenariniame posėdyje data	AFET 21.1.2021	ECON 21.1.2021	IMCO 21.1.2021	TRAN 21.1.2021
	CULT 21.1.2021	LIBE 21.1.2021		
Nuomonė nepareikšta Sprendimo data	ECON 26.1.2021	CULT 11.1.2021		
Susiję komitetai Paskelbimo plenariniame posėdyje data	LIBE 20.5.2021			
Pranešėjai Paskyrimo data	Bart Groothuis 14.1.2021			
Svarstymas komitete	13.4.2021	26.5.2021		
Priėmimo data	28.10.2021			
Galutinio balsavimo rezultatai	+: –: 0:	70 3 1		
Posėdyje per galutinį balsavimą dalyvavę nariai	Nicola Beer, François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Vasile Blaga, Michael Bloss, Manuel Bompard, Paolo Borchia, Marc Botenga, Markus Buchheit, Cristian-Silviu Buşoi, Carlo Calenda, Maria da Graça Carvalho, Ignazio Corrao, Ciarán Cuffe, Josianne Cutajar, Nicola Danti, Pilar del Castillo Vera, Christian Ehler, Valter Flego, Niels Fuglsang, Lina Gálvez Muñoz, Claudia Gamon, Bart Groothuis, Christophe Grudler, András Gyürk, Henrike Hahn, Robert Hajšel, Ivo Hristov, Ivars Ijabs, Romana Jerković, Eva Kaili, Seán Kelly, Izabela-Helena Kloc, Łukasz Kohut, Zdzisław Krasnodębski, Andrius Kubilius, Miapetra Kumpula-Natri, Thierry Mariani, Marisa Matias, Eva Maydell, Georg Mayer, Joëlle Mélin, Dan Nica, Angelika Niebler, Ville Niinistö, Aldo Patriciello, Mauri Pekkarinen, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Clara Ponsatí Obiols, Manuela Ripa, Robert Roos, Sara Skyttedal, Maria Spyraki, Jessica Stegrud, Beata Szydło, Riho Terras, Grzegorz Tobiszowski, Isabella Tovaglieri, Viktor Uspaskich, Henna Virkkunen, Pernille Weiss, Carlos Zorrinho			
Posėdyje per galutinį balsavimą dalyvavę pavaduojantys nariai	Rasmus Andresen, Marek Paweł Balt, Klemen Grošelj, Adam Jarubas, Elena Lizzi, Adriana Maldonado López, Bronis Ropė, Jordi Solé, Nils Torvalds			
Pateikimo data	4.11.2021			

GALUTINIS VARDINIS BALSAVIMAS ATSAKINGAME KOMITETE

70	+
ECR	Izabela-Helena Kloc, Zdzisław Krasnodębski, Robert Roos, Beata Szydło, Grzegorz Tobiszowski
ID	Paolo Borchia, Markus Buchheit, Elena Lizzi, Thierry Mariani, Georg Mayer, Joëlle Mélin, Isabella Tovaglieri
NI	András Gyürk, Clara Ponsatí Obiols, Viktor Uspaskich
PPE	François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Vasile Blaga, Cristian-Silviu Buşoi, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Adam Jarubas, Seán Kelly, Andrius Kubilius, Eva Maydell, Angelika Niebler, Aldo Patriciello, Markus Pieper, Sara Skyttedal, Maria Spyraki, Riho Terras, Henna Virkkunen, Pernille Weiss
RENEW	Nicola Beer, Nicola Danti, Valter Flego, Claudia Gamon, Bart Groothuis, Klemen Grošelj, Christophe Grudler, Ivars Ijabs, Mauri Pekkarinen, Morten Petersen, Nils Torvalds
S&D	Marek Paweł Balt, Carlo Calenda, Josianne Cutajar, Niels Fuglsang, Lina Gálvez Muñoz, Robert Hajšel, Ivo Hristov, Romana Jerković, Eva Kaili, Łukasz Kohut, Miapetra Kumpula-Natri, Adriana Maldonado López, Dan Nica, Tsvetelina Penkova, Carlos Zorrinho
Verts/ALE	Rasmus Andresen, Michael Bloss, Ignazio Corrao, Ciarán Cuffe, Henrike Hahn, Ville Niinistö, Manuela Ripa, Bronis Ropė, Jordi Solé

3	-
The Left	Manuel Bompard, Marc Botenga, Marisa Matias

1	0
ECR	Jessica Stegrud

Sutartiniai ženklai:
+ : už
- : prieš
0 : susilaikė