



Briuselis, 2021 m. lapkričio 26 d.
(OR. en)

14337/21

Tarpinstitucinė byla:
2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

PRANEŠIMAS

nuo: Tarybos generalinio sekretoriato
kam: Tarybai

Ankstesnio
dokumento Nr.: 9583/2/21, 11724/21
Komisijos dok. Nr.: 14150/20

Dalykas: Pasiūlymas dėl Europos Parlamento ir Tarybos direktyvos dėl priemonių
aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti,
kuria panaikinama Direktyva (ES) 2016/1148
– *Bendras požiūris*

I. IVADAS

1. 2020 m. gruodžio 16 d. Komisija priėmė pasiūlymą dėl Direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti (peržiūrėta TIS direktyva arba TIS 2)¹, kuria siekiama pakeisti galiojančią Direktyvą dėl tinklų ir informacinių sistemų saugumo (TIS direktyva)².

¹ Pasiūlymas dėl Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148.

² 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.

Pasiūlymas buvo vienas iš veiksmų, numatytų ES skaitmeninio dešimtmečio kibernetinio saugumo strategijoje³, siekiant užtikrinti, kad piliečiai ir įmonės galėtų pasinaudoti patikimomis skaitmeninėmis technologijomis.

2. Pasiūlymas grindžiamas Sutarties dėl Europos Sąjungos veikimo (SESV) 114 straipsniu ir juo siekiama dar labiau padidinti viešųjų ir privačiųjų subjektų, kompetentingų institucijų ir visos Sąjungos atsparumą ir reagavimo į incidentus pajėgumus.
3. Europos Parlamente už pasiūlymą atsakingas Pramonės, mokslinių tyrimų ir energetikos komitetas (ITRE). ITRE komitetas pranešėjo pranešimą priėmė 2021 m. spalio 28 d.
4. Europos ekonomikos ir socialinių reikalų komitetas nuomonę priėmė 2021 m. balandžio 28 d.
5. 2021 m. vasario 3 d. Nuolatinų atstovų komitetas nusprendė dėl pasiūlymo pasikonsultuoti su Europos regionų komitetu⁴. Iki šiol Europos regionų komitetas savo nuomonės nepateikė.
6. Europos duomenų apsaugos priežiūros pareigūnas nuomonę priėmė 2021 m. kovo 11 d.⁵
7. 2021 m. kovo 22 d. išvadose dėl ES skaitmeninio dešimtmečio kibernetinio saugumo strategijos⁶ Taryba atkreipė dėmesį į naują pasiūlymą, kuris grindžiamas TIS direktyva, ir pakartojo remianti nacionalinių kibernetinio saugumo sistemų stiprinimą ir derinimą bei nuolatinį valstybių narių bendradarbiavimą.
8. 2021 m. spalio 21–22 d. išvadose Europos Vadovų Taryba paragino paspartinti darbą, susijusį su pasiūlymu dėl peržiūrėtos TIS direktyvos.

³ Dok. 14133/20.

⁴ Dok. 5573/21.

⁵ Nuomonė 5/2021 dėl kibernetinio saugumo strategijos ir TIS 2.0 direktyvos.

⁶ Dok. 6722/21.

II. TARYBOS PARENGIAMŲJŲ ORGANŲ DARBAS

9. Taryboje pasiūlymą nagrinėja Kibernetinių klausimų horizontalioji darbo grupė (HWPCI). Pasiūlymas pradėtas nagrinėti sausio 19 d. Portugalijos pirmininkavimo laikotarpiu – jis išsamiai apsvaistytas, kad valstybės narės galėtų pateikti savo klausimus ir akcentuoti pagrindinius joms rūpimus klausimus, taip pat gauti išsamius Komisijos paaiškinimus, susijusius su peržiūrėtos direktyvos pakeitimais.
10. Portugalijos pirmininkavimo laikotarpiu HWPCI šio pasiūlymo pristatymui ir svarstymui skyrė 17 posėdžių. Svarstymo pažangos ataskaita buvo pateikta 2021 m. birželio 4 d. TTE tarybos posėdyje.
11. Po to, Slovėnijos pirmininkavimo laikotarpiu darbas buvo tęsiamas ir suintensyvėjo siekiant susitarti dėl bendro požiūrio 2021 m. gruodžio 3 d. Tarybos (transportas, telekomunikacijos ir energetika) posėdyje. Pirmininkaujanti Slovėnija TIS 2 pasiūlymo peržiūrai skyrė 15 posėdžių ir surengė daug dvišalių diskusijų visais lygmenimis.
12. Atlikdama savo darbą HWPCI daugiausia dėmesio skyrė pasiūlymo teksto performulavimui, pirmiausia, TIS 2 direktyvos sąveikai su sektorių teisės aktais ir taikymo sričiai, ypač kiek tai susiję su viešuoju administravimu, domenų vardų sistemos šakniniais serveriais ir netaikymo sąlyga, taip pat, be kita ko, tarpusavio vertinimams, jurisdikcijai ir savitarpio pagalbai, suderintam pažeidžiamumų atskleidimui, domenų vardų ir registracijos duomenų bazėms ir tarptautiniam bendradarbiavimui.
13. Pirmasis kompromisinis pasiūlymas dėl siūlomos direktyvos teksto buvo paskelbtas 2021 m. rugsėjo 21 d.⁷; jis buvo grindžiamas valstybių narių rašytinėmis pastabomis ir neoficialiais dokumentais, taip pat ankstesniais kompromisiniais pasiūlymais dėl TIS 2 direktyvos sąveikos su sektorių teisės aktais ir dėl TIS 2 direktyvos taikymo srities.

⁷ Dok. 12019/21.

14. Naujausia pirmininkaujančios valstybės narės kompromisinio pasiūlymo redakcija⁸ darbo grupės lygmeniu svarstyta 2021 m. lapkričio 22 d. Delegacijos iš esmės palankiai įvertino kompromisinį tekstą, tačiau dėl kompromisinio pasiūlymo dalių dar buvo pareikštos kelios tikrinimo išlygos ar pateikta pastabų. Dar buvo pasiūlyta atlikti kai kuriuos techninius tam tikrų teksto dalių redakcinius pakeitimus.

III. ESMĖ

15. Remiantis diskusijų darbo grupės lygmeniu rezultatais identifikuoti šie pagrindiniai politiniai klausimai:

a) Taikymo sritis (2 straipsnis)

Tik prasidėjus diskusijoms dėl TIS 2 pasiūlymo, pagrindiniai valstybių narių pareikšti susirūpinimą kėlę klausimai buvo susiję su labai išaugusiu subjektų, kuriems taikoma direktyva, skaičiumi, ypač su dydžio ribos taisyklės nustatymu, kurios laikantis į direktyvos taikymo sritį įtraukiami visi vidutinio dydžio ir dideli subjektai, veikiantys sektoriuose arba teikiantys paslaugas, kurioms taikoma TIS 2 direktyva. Kompromisiniame pasiūlyme išlaikyta ši bendra taisyklė, tačiau į ją įtrauktos papildomos nuostatos siekiant užtikrinti būtiną proporcingumą, didesnę rizikos valdymo lygį ir aiškiai apibrėžtus ypatingos svarbos kriterijus, kuriais remiantis būtų nustatoma, ar subjektai patenka į direktyvos taikymo sritį. Be to, į kompromisinį pasiūlymą įtrauktos konkrečios nuostatos dėl priežiūros priemonių naudojimo išdėstymo pagal prioritetus remiantis rizika grindžiamu požiūriu.

⁸ Dok. 12019/5/21 REV 5.

b) Viešasis administravimas (2 straipsnio 2a dalis)

Viešojo administravimo įtraukimas į TIS 2 direktyvos taikymo sritį buvo labai aktyviai aptarta tema, nes laikytasi nuomonės, kad viešojo administravimo sektorius yra labiau išskirtinis nei kiti sektoriai, kuriems taikoma TIS 2 direktyva. Pirmininkaujanti valstybė narė siekė subalansuoto požiūrio, kuriame būtų atsižvelgta į nacionalinių viešojo administravimo sistemų ypatumus ir užtikrinta, kad valstybėms narėms būtų suteikta tam tikro lankstumo nustatant viešojo administravimo subjektus, kuriems taikoma TIS 2. Todėl kompromisiniame tekste TIS 2 taikoma centrinės valdžios viešojo administravimo subjektams, o valstybės narės gali taip pat nustatyti, kad direktyva būtų taikoma viešojo administravimo subjektams regionų ar vietos lygmeniu.

c) Netaikymo nuostata (2 straipsnio 3a ir 3aa punktai)

Valstybės narės pageidavo, kad netaikymo nuostata būtų išsamiau paaiškinta nustatant, kad direktyva netaikoma subjektams, kurie daugiausia vykdo veiklą gynybos, nacionalinio saugumo, visuomenės saugumo ar teisėsaugos srityse arba veiklą, susijusią su nacionaliniu saugumu arba gynyba. Ji taip pat netaikoma teisminėmis institucijoms, parlamentams ir centriniais bankams.

d) Sąveika su sektorių teisės aktais

Valstybės narės pabrėžė, kad TIS 2 direktyvą reikia suderinti su sektorių teisės aktais, visų pirma su Reglamentu dėl skaitmeninės veiklos atsparumo finansų sektoriuje (DORA) ir Direktyva dėl ypatingos svarbos subjektų atsparumo (CER direktyva). TIS 2 direktyvoje, kuri turėtų būti būtino suderinimo kibernetinio saugumo srityje pagrindas, yra specialus straipsnis dėl konkrečioms sektoriams taikomų Sąjungos aktų (2b straipsnis). Kalbant apie sąveiką su CER direktyva, kompromisiniu pasiūlymu užtikrinamas didesnis aiškumas dėl visų rūšių pavojus apimančio požiūrio. Kiti svarbūs papildymai yra susiję su kompetentingų institucijų bendradarbiavimo susitarimais pagal atitinkamus teisės aktus.

e) Tarpusavio vertinimai (16 straipsnis)

Su tam tikromis išimtimis valstybės narės prieštaravo tam, kad Komisija nustatytų privalomus tarpusavio vertinimus. Siūlomu kompromisu užtikrinama, kad naujasis tarpusavio vertinimo mechanizmas būtų grindžiamas tarpusavio pasitikėjimu ir būtų savanoriškas bei pačių valstybių narių vykdomas procesas.

f) Jurisdikcija ir teritoriškumas (24 straipsnis) ir savitarpio pagalba (34 straipsnis)

Valstybės narės pareiškė susirūpinimą dėl Komisijos pasiūlyto diferencijuotos jurisdikcijos taikymo IRT sektoriaus subjektams pasekmių. Kompromisiniame tekste paaiškintas jurisdikcijos taikymas atsižvelgiant į subjektų rūšį, taip pat sugriežtinta formuluotė dėl savitarpio pagalbos.

g) Pareigos pranešti (20 straipsnis)

Atsižvelgiant į valstybių narių pareikštą susirūpinimą, kad dėl to subjektams, kuriems taikoma TIS 2 direktyva, tektų pernelyg didelė našta ir būtų teikiama per daug pranešimų, iš kompromisinio teksto išbrauktas privalomas pranešimas apie dideles kibernetines grėsmes.

IV. IŠVADA

16. 2021 m. lapkričio 24 d. Nuolatinių atstovų komitetas pasiekė susitarimą dėl priede išdėstyto kompromisinio teksto ir nusprendė jį perduoti Tarybai (transportas, telekomunikacijos ir energetika), kad būtų priimtas bendras požiūris.
17. Todėl Tarybos prašoma patvirtinti priede pateiktą pirmininkaujančios valstybės narės parengtą kompromisinį tekstą ir 2021 m. gruodžio 3 d. posėdyje priimti bendrą požiūrį.

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA

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

(Tekstas svarbus EEE)

EUROPOS PARLAMENTAS IR EUROPOS SĄJUNGOS TARYBA,

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

atsižvelgdami į Europos Komisijos pasiūlymą,

teisėkūros procedūra priimamo akto projektą perdavus nacionaliniams parlamentams,

atsižvelgdami į Europos ekonomikos ir socialinių reikalų komiteto nuomonę⁹,

atsižvelgdami į Regionų komiteto nuomonę¹⁰,

laikydami įprastos teisėkūros procedūros,

OL C [...], [...], p. [...].

OL C [...], [...], p. [...].

kadangi:

- (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 veiksmingo Sąjungos ekonomikos ir visuomenės veikimo;
- (2) nuo Direktyvos (ES) 2016/1148 įsigaliojimo padaryta didelė pažanga didinant Sąjungos kibernetinio atsparumo lygį. Persvarsčius tą direktyvą, paaiškėjo, kad ji tapo institucinio ir reguliavimo požiūrio į kibernetinį saugumą Sąjungoje paskata ir sudarė sąlygas reikšmingam mąstysenos pokyčiui. Ta direktyva padėjo galutinai sukurti nacionalines sistemas apibrėžiant nacionalines [...] **tinklų ir informacinių sistemų 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 grupę¹² ir sukuriant nacionalinių reagavimo į kompiuterinius saugumo incidentus tarnybų tinklą (CSIRT tinklą)¹³. Nepaisant šių laimėjimų, peržiūrėjus Direktyvą (ES) 2016/1148 paaiškėjo jos trūkumai, trukdantys veiksmingai spręsti dabartines ir naujas kibernetinio saugumo problemas;

¹¹ 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (OL L 194/1, 2016 7 19, p. 1).

¹² Direktyvos (ES) 2016/1148 11 straipsnis.

¹³ Direktyvos (ES) 2016/1148 12 straipsnis.

- (3) tinklų ir informacinės sistemos dėl sparčios skaitmeninės transformacijos ir visuomenės tarpusavio junglumo, įskaitant tarpvalstybinius mainus, tapo pagrindiniu kasdienio gyvenimo aspektu. Dėl tokių pokyčių grėsmių kibernetiniam saugumui padėtis tapo sudėtingesnė, atsirado naujų problemų, į kurias visos valstybės narės turi reaguoti prisitaikydamos, koordinuotai ir naujoviškai. Kibernetinio saugumo incidentų skaičius, mastas, sudėtingumas, dažnumas ir poveikis didėja ir kelia didelę grėsmę tinklų ir informacinių sistemų veikimui. Todėl kibernetiniai incidentai gali trukdyti vykdyti ekonominę veiklą vidaus rinkoje, sukelti finansinių nuostolių, pakirsti naudotojų pasitikėjimą ir padaryti didelę žalą Sąjungos ekonomikai ir visuomenei. Todėl kibernetinio saugumo parengtis ir veiksmingumas kaip niekad anksčiau yra labai svarbūs tinkamam vidaus rinkos veikimui;
- (4) Direktyvos (ES) 1148/2016 teisinis pagrindas buvo Sutarties dėl Europos Sąjungos veikimo (SESV) 114 straipsnis, kurio tikslas – tobulinant nacionalinių taisyklių suderinimo priemones sukurti vidaus rinką ir užtikrinti jos veikimą. Paslaugas teikiantiems arba svarbią ekonominę veiklą vykdančioms subjektams nustatyti kibernetinio saugumo reikalavimai valstybėse narės gerokai skiriasi atsižvelgiant į reikalavimo rūšį, jų išsamumo lygį ir priežiūros metodą. Dėl šių skirtumų patiriama papildomų išlaidų, o prekes ar paslaugas tarpvalstybiniu mastu tiekiančioms įmonėms kyla sunkumų. Vienos valstybės narės nustatyti reikalavimai, kurie skiriasi nuo kitos valstybės narės nustatytų reikalavimų arba net jiems prieštarauja, gali daryti didelį neigiamą poveikį šiai tarpvalstybinei veiklai.

Be to, tikėtina, kad dėl nepakankamai optimalios kibernetinio saugumo [...] **priemonių** struktūros arba įgyvendinimo vienoje valstybėje narėje kils pasekmių kitų valstybių narių kibernetinio saugumo lygiui, visų pirma atsižvelgiant į intensyviuosius tarpvalstybinius mainus. Peržiūrėjus Direktyvą (ES) 2016/1148, paaiškėjo, kad valstybėse narėse ji įgyvendinama labai įvairiai, be kita ko, skiriasi jos taikymo sritis, nes jos ribų nustatymo klausimas iš esmės buvo paliktas valstybių narių diskrecijai. Direktyva (ES) 2016/1148 valstybėms narėms taip pat buvo suteikta labai plati diskrecija įgyvendinti joje nustatytas saugumo pareigas ir pareigas pranešti apie incidentus. Todėl šios pareigos nacionaliniu lygmeniu buvo įgyvendintos gana skirtingai. Panašūs skirtumai nustatyti direktyvos nuostatų dėl priežiūros ir vykdymo užtikrinimo įgyvendinimo srityje;

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

- (6) [...] valstybės narės **turėtų galėti** imtis priemonių, būtinų gyvybiniais jų saugumo interesams užtikrinti, viešajai tvarkai palaikyti bei visuomenės saugumui užtikrinti, ir sudaryti sąlygas tirti bei išsiaiškinti nusikalstamas veikas ir už jas patraukti baudžiamojon atsakomybėn [...]. [...] **Direktyva turėtų būti netaikoma tam tikriems viešiesiems arba privatiesiems subjektams, vykdančioms veiklą šiose srityse. Ji taip pat turėtų būti netaikoma subjektų šiose srityse vykdomai veiklai. Be to, jokia valstybė narė neturi būti įpareigota teikti informaciją, kurios atskleidimas, jos nuomone, prieštarautų esminiams jos viešojo saugumo interesams. [...] Nacionalinės [...] arba Sąjungos taisyklės dėl įslaptintos informacijos apsaugos, susitarimai dėl informacijos neatskleidimo ir neoficialūs susitarimai dėl informacijos neatskleidimo, pavyzdžiui, Srauto kontrolės protokolas¹⁴;**
- (6a) **pagal šią direktyvą vykdomam asmens duomenų tvarkymui taikoma Sąjungos teisė dėl asmens duomenų ir privatumo apsaugos. Visų pirma ši direktyva nedaro poveikio Europos Parlamento ir Tarybos reglamentui (ES) 2016/679 ir Direktyvai 2002/58/EB, todėl visų pirma turėtų nedaryti poveikio nepriklausomų priežiūros institucijų, kompetentingų stebėti, kaip laikomasi atitinkamų Sąjungos duomenų apsaugos teisės aktų, užduotims ir įgaliojimams;**

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).

- (7) panaikinus Direktyvą (ES) 2016/1148, taikymo sritis sektoriams, atsižvelgiant į 4–6 konstatuojamosiose dalyse išvardytas aplinkybes, turėtų būti praplėsta, kad apimtų platesnį ekonomikos veiklų spektrą. Todėl sektorių, kuriems taikoma Direktyva (ES) 2016/1148, sąrašas turėtų būti papildytas, kad direktyva būtų visapusiškai taikoma sektoriams ir paslaugoms, kurie yra gyvybiškai svarbūs pagrindinei visuomeninei ir ekonominei veiklai vidaus rinkoje. Taisyklės neturėtų skirtis priklausomai nuo to, ar subjektai yra esminių paslaugų operatoriai, ar skaitmeninių paslaugų teikėjai. Iš tiesų tokia diferenciacija yra pasenusi, nes neatspindi faktinės sektorių arba paslaugų svarbos visuomeninei ir ekonominei veiklai vidaus rinkoje;
- (8) pagal Direktyvą (ES) 2016/1148 valstybės narės turėjo pareigą nustatyti, kurie subjektai atitinka esminių paslaugų operatoriams taikomus kriterijus (nustatymo procesas). Šiuo atžvilgiu siekiant pašalinti didelius valstybių narių skirtumus ir užtikrinti rizikos valdymo reikalavimų ir pareigų pranešti teisinį tikrumą visų subjektų atžvilgiu, turėtų būti nustatytas vienas kriterijus, kuriuo remiantis nustatomi subjektai, kurie patenka į šios direktyvos taikymo sritį. Tas kriterijus turėtų būti grindžiamas dydžio ribos taisykle, pagal kurią į direktyvos taikymo sritį patenka visos vidutinės ir didelės įmonės, kaip apibrėžta Komisijos rekomendacijoje 2003/361/EB¹⁵, veikiančios sektoriuose arba teikiančios atitinkamos rūšies paslaugas, kurioms taikoma ši direktyva; [...]

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).

- (8a) siekiant užtikrinti aiškią subjektų, kuriems taikoma ši direktyva, apžvalgą, valstybės narės turėtų galėti nustatyti nacionalinius pranešimo apie save mechanizmus, pagal kuriuos būtų reikalaujama, kad subjektai, kuriems taikoma ši direktyva, pagal šią direktyvą kompetentingoms institucijoms arba šiuo tikslu valstybių narių paskirtiems organams pateiktų bent savo vardą ir pavardę (pavadinimą), adresą ir kontaktinius duomenis, taip pat nurodytų sektorių, kuriame jie veikia, ir paslaugų, kurias jie teikia, rūši, taip pat, kai taikytina, valstybių narių, kuriose tas subjektas teikia savo paslaugas, sąrašą. Valstybės narės gali nuspręsti dėl tinkamų mechanizmų, jei nacionaliniu lygmeniu esama registrų, kurie sudarytų sąlygas nustatyti subjektus, kurie patenka į šios direktyvos taikymo sritį;
- (9) [...] šios direktyvos taikymo sritį taip pat turėtų pateikti **labai maži** arba mažieji [...] 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 būti atsakingos [...] už tai, kad [...] Komisijai būtų pateikta bent atitinkama informacija apie nustatytų subjektų skaičių, sektorių, kuriame jie veikia, arba paslaugų, kurias jie teikia, rūšis, taip pat konkrečius kriterijus, kuriais remiantis jie buvo nustatyti. Laikydamosi nacionalinių saugumo taisyklių valstybės narės taip pat gali nuspręsti pateikti Komisijai šių subjektų vardus ir pavardes (pavadinimus);
- (9a) viešojo administravimo subjektams, vykdančioms veiklą nacionalinio saugumo, gynybos, visuomenės saugumo, teisėsaugos, taip pat su teisminėmis institucijoms, parlamentais ir centriniais bankais susijusiose srityse, ši direktyva netaikoma. Šios direktyvos tikslais kompetenciją reglamentavimo srityje turintys subjektai nelaikomi subjektais, vykdančiais veiklą teisėsaugos srityje, todėl dėl šių priežasčių ši direktyva jiems yra taikoma. Be to, ši direktyva netaikoma centrinės valdžios viešojo administravimo subjektams, įsteigtiems kartu su trečiąja valstybe pagal tarptautinį susitarimą;

- (9aa) valstybės narės turėtų galėti nustatyti, kad subjektai, kurie prieš šios direktyvos įsigaliojimą buvo įvardyti kaip esminių paslaugų operatoriai pagal Direktyvą (ES) 2016/1148, būtų laikomi esminiais subjektais;
- (9aaa) ši direktyva netaikoma valstybių narių diplomatinėms atstovybėms bei konsulinėms įstaigoms užsienyje ir jų naudojamai IRT infrastruktūrai, jei tokia infrastruktūra yra užsienyje arba yra jei ji eksploatuojama užsienyje esantiems naudotojams;
- (10) Komisija, bendradarbiaudama su Bendradarbiavimo grupe, gali paskelbti labai mažoms ir mažosioms įmonėms taikomų kriterijų įgyvendinimo gaires;
- (11) [...]subjektai, kuriems taikoma ši direktyva, turėtų būti skirstomi į dvi kategorijas: esminių ir svarbių subjektų, atsižvelgiant į sektoriaus arba jų teikiamų paslaugų rūšies svarbos lygį, taip pat jų dydį. Šiuo atžvilgiu, kai taikytina, taip pat turėtų būti tinkamai atsižvelgiama į visus atitinkamus kompetentingų institucijų atliktus sektorių rizikos vertinimus ar pateiktas gaires. Tiek esminiams, tiek svarbiems subjektams turėtų būti taikomi [...] rizikos valdymo reikalavimai ir pareigos pranešti. Abiejų kategorijų subjektams taikomi priežiūros ir sankcijų režimai turėtų būti diferencijuojami siekiant užtikrinti tinkamą, viena vertus, **rizika grindžiamų** reikalavimų ir pareigų ir, kita vertus, administracinės naštos, atsirandančios dėl atitikties priežiūros, pusiausvyrą;

- (12) šioje direktyvoje nustatomi kibernetinio saugumo rizikos valdymo priemonių pagrindai ir pareigos pranešti, taikomi visuose į jos taikymo sritį patenkančiuose sektoriuose. Siekiant išvengti Sąjungos teisės aktų nuostatų dėl kibernetinio saugumo susiskaidymo, kai manoma, jog yra būtinos papildomos konkretiems sektoriams taikomos nuostatos, susijusios su kibernetinio saugumo rizikos valdymo priemonėmis ir pareigomis pranešti, siekiant užtikrinti aukšto lygio kibernetinį saugumą, Komisija turėtų įvertinti, ar tokios nuostatos galėtų būti nustatytos pagal šioje direktyvoje numatytus įgaliojimus priimtame įgyvendinimo akte. Jei tokie aktai būtų netinkami tam tikslui, konkretiems sektoriams taikomi teisės aktai galėtų padėti užtikrinti aukšto lygio [...] kibernetinį saugumą, visapusiškai atsižvelgiant į [...] atitinkamų sektorių specifiką ir sudėtingumą. **Konkreiems sektoriams taikomuose teisės aktuose turi būti paaiškinti motyvai, kodėl pagal šioje direktyvoje numatytus įgaliojimus priimtas įgyvendinimo aktas laikomas netinkamu. Kartu tokiose konkretiems sektoriams taikomų Sąjungos teisės aktų nuostatose turėtų būti tinkamai atsižvelgta į poreikį sukurti visapusišką ir suderintą kibernetinio saugumo sistemą. [...] Tai [...] nedaro poveikio dabartiniams įgyvendinimo įgaliojimams, kurie Komisijai yra suteikti įvairiuose sektoriuose, įskaitant transporto ir energetikos sektorius;**

(12a) jeigu konkrečiam sektoriui taikomame Sąjungos teisės akte yra nuostatų, [...] pagal kurias reikalaujama, kad esminiai ar svarbūs subjektai patvirtintų priemonės, kurių poveikis būtų bent lygiavertis šioje direktyvoje nustatytiems pareigoms, susijusioms su kibernetinio saugumo valdymu, [...] ir pareigomis pranešti apie didelius incidentus arba dideles kibernetines grėsmes [...], turėtų būti taikomos tos konkrečiam sektoriui skirtos nuostatos, įskaitant priežiūrą ir vykdymo užtikrinimą reglamentuojančias nuostatas. Nustatant konkrečiam sektoriui taikomo Sąjungos teisės akto nuostatose išdėstytų pareigų lygiavertį poveikį turėtų būti atsižvelgiama į šiuos aspektus: i) kibernetinio saugumo rizikos valdymo priemonės turėtų sudaryti tinkamos ir proporcingos techninės bei organizacinės priemonės, skirtos tinklų ir informacinių sistemų, kurias naudoja atitinkami subjektai teikdami savo paslaugas, saugumui kylančiai rizikai valdyti, ir į jas turėtų būti įtraukti bent visi šioje direktyvoje nustatyti elementai; ii) prievolė pranešti apie didelius incidentus ir kibernetines grėsmes turėtų būti bent lygiavertė šioje direktyvoje nustatytiems pareigoms, susijusioms su pranešimų turiniu, forma ir terminais; iii) subjektų ir atitinkamų valdžios institucijų, atsakingų už konkrečiams sektoriams taikomus Sąjungos teisės aktus, pranešimų teikimo sąlygos turėtų būti bent lygiavertės šioje direktyvoje nustatytiems reikalavimams, susijusiems su jų turiniu, forma bei terminais, ir jose turėtų būti atsižvelgiama į CSIRT vaidmenį; iv) atitinkamų valdžios institucijų tarpvalstybinio bendradarbiavimo reikalavimai turėtų būti bent lygiaverčiai šioje direktyvoje nustatytiems reikalavimams. Jei konkrečiam sektoriui taikomo Sąjungos teisės akto nuostatos neapima visų konkretaus sektoriaus, kuriam taikoma ši direktyva, subjektų, šiems subjektams, kuriems netaikomos tos konkrečiam sektoriui skirtos nuostatos, turėtų būti toliau taikomos atitinkamos šios direktyvos nuostatos;

- (12aa) Komisija turėtų periodiškai peržiūrėti lygiavertį poveikį turinčių reikalavimų taikymą, kiek tai susiję su konkrečioms sektoriams taikomų Sąjungos teisės aktų nuostatomis [...]. Rengdama periodinę peržiūrą Komisija turi konsultuotis su Bendradarbiavimo grupe;**
- (12aaa) būsimuose konkrečioms sektoriams taikomuose Sąjungos teisės aktuose turėtų būti tinkamai atsižvelgiama į šios direktyvos 4 straipsnyje pateiktas apibrėžtis ir į šios direktyvos VI skyriuje nustatytą priežiūros ir vykdymo užtikrinimo sistemą;**
- (12ab) jeigu pagal konkrečioms sektoriams taikomų Sąjungos teisės aktų nuostatas reikalaujama, kad esminiai ar svarbūs subjektai patvirtintų priemones, kurių poveikis būtų bent lygiavertis šioje direktyvoje nustatytoms pareigoms pranešti, turėtų būti vengiama pareigų pranešti dubliavimosi ir turėtų būti užtikrintas pranešimų apie kibernetines grėsmes ar incidentus tvarkymo nuoseklumas ir efektyvumas. Šiuo tikslu pagal tas konkrečiam sektoriui skirtas nuostatas valstybės narės gali būti leidžiama sukurti bendrą, automatinį tiesioginio pranešimo mechanizmą, naudotiną pranešti apie didelius incidentus ir kibernetines grėsmes atitinkamai tiek valdžios institucijoms, kurių užduotys yra nustatytos atitinkamose konkrečioms sektoriams skirtose nuostatose, tiek kompetentingoms institucijoms, įskaitant bendrąjį informacinį centrą ir CSIRT, atsakingus už šioje direktyvoje numatytas kibernetinio saugumo užduotis, arba mechanizmą, kuriuo būtų užtikrinamas atitinkamų valdžios institucijų ir CSIRT sistemingas ir neatidėliotinas dalijimasis informacija ir bendradarbiavimas tokių pranešimų tvarkymo srityje. Siekiant supaprastinti pranešimų teikimą ir įgyvendinti bendrą, automatinį tiesioginio pranešimo mechanizmą, laikydamosi konkrečioms sektoriams taikomų teisės aktų valstybės narės gali naudotis viena bendra prieiga, kurią jos sukuria pagal šios direktyvos 11 straipsnio 5a dalį. Siekiant užtikrinti suderinimą, konkrečioms sektoriams taikomuose Sąjungos teisės aktuose nustatytos pareigos pranešti turėtų būti suderintos su šioje direktyvoje nustatytais pareigomis. Valstybės narės gali nustatyti, kad pagal šią direktyvą kompetentingos institucijos arba nacionalinės CSIRT būtų pranešimų gavėjos pagal konkrečioms sektoriams taikomus teisės aktus;**

- (13) atsižvelgiant į tai, kiek ši direktyva yra susijusi su finansų sektoriaus subjektais, Europos Parlamento ir Tarybos reglamentas XXXX/XXXX turėtų būti vertinamas kaip konkrečiam sektoriui taikomas Sąjungos teisės aktas. Reglamento XXXX/XXXX nuostatos, susijusios su informacinių ir ryšių technologijų (IRT) rizikos valdymo priemonėmis, su IRT susijusių incidentų valdymu, ypač pranešimu apie incidentus, taip pat su skaitmeninės veiklos atsparumo testavimu, dalijimosi informacija tvarka ir trečiosios šalies IRT rizika, turėtų būti taikomos vietoj šioje direktyvoje nustatytų reikalavimų. Todėl valstybės narės šios direktyvos nuostatų dėl kibernetinio saugumo rizikos valdymo [...], pareigų pranešti ir [...] priežiūros bei vykdymo užtikrinimo turėtų netaikyti [...] finansų sektoriaus subjektams, kuriems taikomas Reglamentas XXXX/XXXX. Kartu pagal šią direktyvą svarbu išlaikyti tvirtus ryšius su finansų sektoriumi ir užtikrinti, kad su juo būtų keičiamasi informacija. Šiuo tikslu Reglamentu XXXX/XXXX [...] Europos finansų sektoriaus priežiūros institucijoms (EPI) ir pagal Reglamentą XXXX/XXXX [...] nacionalinėms kompetentingoms institucijoms leidžiama dalyvauti [...] Bendradarbiavimo grupės [...] **darbe**, taip pat keistis informacija bei bendradarbiauti su pagal šią direktyvą paskirtais bendraisiais informaciniais centrais, [...] **taip pat** su nacionalinėmis CSIRT. Pagal Reglamentą XXXX/XXXX kompetentingos institucijos išsamius duomenis apie didelius su IRT susijusius incidentus **ir dideles kibernetines grėsmes** taip pat turėtų perduoti pagal šią direktyvą paskirtiems bendriesiems informaciniams centrams, **kompetentingoms institucijoms ar nacionalinėms CSIRT. Tai galima daryti automatiškai ir tiesiogiai perduodant pranešimus apie incidentus arba naudojantis bendra pranešimų teikimo platforma.** Be to, valstybės narės į savo kibernetinio saugumo strategijas turėtų toliau įtraukti finansų sektorių, o nacionalinės CSIRT savo veikloje gali aptarti finansų sektoriaus klausimus;

(13a) siekiant išvengti spragų tarp kibernetinio saugumo pareigų, nustatytų I priedo 2 punkto a papunktyje nurodytiems aviacijos sektoriaus subjektams, ir šių pareigų dubliavimosi, pagal Europos Parlamento ir Tarybos reglamentus (EB) Nr. 300/2008¹⁶ ir (ES) 2018/1139¹⁷ paskirtos nacionalinės institucijos ir pagal šią direktyvą kompetentingos institucijos turėtų bendradarbiauti įgyvendindamos kibernetinio saugumo rizikos valdymo priemonės ir vykdydamos tų priemonių priežiūrą nacionaliniu lygmeniu. Tai, kad subjektas laikosi pagal šią direktyvą nustatytų kibernetinio saugumo rizikos valdymo priemonių, [...] pagal reglamentus (EB) Nr. 300/2008 ir (ES) 2018/1139 paskirtos nacionalinės institucijos gali pripažinti, kad jie laikosi ir šiuose reglamentuose bei atitinkamuose pagal tuos reglamentus priimtuose deleguotuosiuose ir įgyvendinimo aktuose nustatytų reikalavimų;

¹⁶ 2008 m. kovo 11 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 300/2008 dėl civilinės aviacijos saugumo bendrųjų taisyklių ir panaikinant Reglamentą (EB) Nr. 2320/2002 (OL L 97, 2008 4 9, p. 72).

¹⁷ 2018 m. liepos 4 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1139 dėl bendrųjų civilinės aviacijos taisyklių, ir kuriuo įsteigiama Europos Sąjungos aviacijos saugos agentūra, iš dalies keičiami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 2111/2005, (EB) Nr. 1008/2008, (ES) Nr. 996/2010, (ES) Nr. 376/2014 ir direktyvos 2014/30/ES ir 2014/53/ES bei panaikinami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 552/2004 ir (EB) Nr. 216/2008 bei Tarybos reglamentas (EEB) Nr. 3922/91 (OL L 212, 2018 8 22, p. 1).

- (14) atsižvelgiant į kibernetinio saugumo ir subjektų fizinio saugumo tarpusavio ryšius, reikėtų užtikrinti nuoseklų požiūrį tarp Europos Parlamento ir Tarybos direktyvos (ES) XXX/XXX ir šios direktyvos. Kad pasiektų šį tikslą, valstybės narės turėtų užtikrinti, kad ypatingos svarbos subjektai, [ir lygiaverčiai 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. **Kompetentingos** [...]institucijos pagal abi direktyvas turėtų bendradarbiauti ir keistis informacija, visų pirma kiek tai susiję su ypatingos svarbos subjektų nustatymu, kibernetinėmis grėsmėmis, kibernetinio saugumo rizika ir incidentais, **taip pat su nekibernetine rizika, grėsmėmis ir incidentais**, darančiais poveikį ypatingos svarbos subjektams [arba **ypatingos svarbos subjektams lygiaverčiams subjektams**], [...] **įskaitant** kibernetinio saugumo **ir fizines** priemones, kurių ėmėsi ypatingos svarbos subjektai, **ir tokių subjektų atžvilgiu vykdomos priežiūros veiklos rezultatais. Be to, siekiant supaprastinti pagal abi direktyvas paskirtų kompetentingų institucijų vykdomą tarpusavio priežiūros veiklą ir kuo labiau sumažinti atitinkamiems subjektams tenkančią administracinę naštą, kompetentingos institucijos turėtų stengtis suderinti pranešimo apie incidentus šablonus ir priežiūros procesus.** [...] **Kai tikslinga**, pagal Direktyvą (ES) XXX/XXX kompetentingos institucijos [...] **gali prašyti, kad** pagal šią direktyvą kompetentingos institucijos [...] įgyvendintų savo priežiūros ir vykdymo užtikrinimo įgaliojimus subjektų, kurie įvardyti kaip ypatingos svarbos subjektai, **atžvilgiu**; [...]

- (14a) skaitmeninės infrastruktūros sektoriaus subjektai iš esmės priklauso nuo tinklų ir informacinių sistemų, todėl pagal šią direktyvą tiems subjektams nustatant pareigas turėtų būti visapusiškai atsižvelgiama į tokių sistemų fizinį saugumą, kaip jų kibernetinio saugumo rizikos valdymo ir pranešimo pareigų dalį. Kadangi tiems klausimams taikoma ši direktyva, Direktyvos (ES) XXX/XXX [CER] III–VI skyriuose nustatytos pareigos tokiems subjektams netaikomos;
- (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 DNS paslaugų teikėjams DNS teikimo ir keitimo grandinėje, kurie yra svarbūs vidaus rinkai, įskaitant [...] aukščiausio lygio domenų (TLD) vardų registrus[...], domenų vardų registravimo paslaugas teikiančius subjektus, patikimų domenų vardų serverių operatorius ir rekursinių keitiklių operatorius. Terminas „DNS paslaugų teikėjas“ turėtų būti netaikomas DNS paslaugoms, kurias savo reikmėms teikia atitinkamas subjektas ir su juo susiję subjektai. Pagal šią direktyvą šios kategorijos paslaugų teikėjams nustatytos kibernetinio saugumo pareigos griežtai apsiriboja kibernetinio saugumo rizikos valdymo priemonėmis ir pranešimų teikimu, todėl jos nedaro poveikio įvairių suinteresuotųjų subjektų bendruomenės vykdomam visuotinių DNS valdymui;

- (16) debesijos kompiuterijos paslaugos turėtų apimti skaitmenines paslaugas, kurios pagal poreikį suteikia plataus masto nuotolinę prieigą prie kintamo masto pritaikomos bendrų kompiuterijos išteklių bazės. Šie kompiuterijos ištekliai apima tokius išteklius, kaip tinklai, serveriai ar kita infrastruktūra, operacinės sistemos, programinė įranga, kaupikliai, taikomosios programos ir paslaugos. **Debesijos kompiuterijos paslaugų modeliai, be kita ko, apima paslauginę infrastruktūrą (IaaS), paslauginę platformą (PaaS), paslauginę programinę įrangą (SaaS) ir paslauginį tinklą (NaaS).** Debesijos kompiuterijos diegimo modeliai turėtų apimti privačią, viešą ir mišrią debesiją. Pirmiau minėti paslaugos ir diegimo modeliai turi tokią pat reikšmę kaip ir pagal ISO/IEC 17788:2014 standartą apibrėžti paslaugos sąlygų ir diegimo modeliai. Debesijos kompiuterijos naudotojo gebėjimas vienašališkai pasirūpinti kompiuterijos pajėgumais, pavyzdžiui, serverio laiku arba tinklo saugykla, be jokio žmogaus įsikišimo ir naudojantis debesijos kompiuterijos paslaugų teikėju, galėtų būti apibūdinamas kaip administravimas pagal poreikį. Terminas „plataus masto nuotolinė prieiga“ naudojama apibūdinant debesijos pajėgumus, kurie užtikrinami tinkle ir kuriais galima pasinaudoti per mechanizmus, kuriais skatinamas įvairių mažafunkčių arba daugiafunkčių kompiuterių platformų (įskaitant mobiliuosius telefonus, planšetinius kompiuterius, knyginius kompiuterius, profesionaliuosius kompiuterius) naudojimas.

Terminas „kintamo masto“ reiškia, kad siekdamas atsižvelgti į paklausos svyravimus, debesijos paslaugų teikėjas lanksčiai paskirsto kompiuterijos išteklius nepriklausomai nuo geografinės išteklių vietos. Terminas „pritaikoma bazė“ reiškia, kad siekiant sparčiai padidinti ir sumažinti tuos turimus kompiuterijos išteklius pagal darbo krūvį, tais ištekliais aprūpinama ir jie yra tiekiami atsižvelgiant į paklausą. Terminas „bendras“ reiškia, kad tie kompiuterijos ištekliai yra tiekiami įvairiems naudotojams, kurie dalijasi bendra prieiga prie paslaugos, tačiau tie ištekliai tvarkomi atskirai kiekvieno naudotojo atveju, nors paslauga yra teikiama naudojant tą pačią elektroninę įrangą. Terminas „paskirstytasis“ reiškia tuos kompiuterijos išteklius, kurie yra skirtinguose tinkliniuose kompiuteriuose ar prietaisuose ir kurie tarpusavyje bendrauja ir koordinuoja perduodami pranešimus;

- (17) atsižvelgiant į novatoriškų technologijų ir naujų verslo modelių atsiradimą, tikimasi, kad rinkoje atsiras naujų debesijos kompiuterijos diegimo ir paslaugų modelių, atsižvelgiant į kintančius vartotojų poreikius. Šiomis aplinkybėmis debesijos kompiuterijos paslaugos gali būti teikiamos labai paskirstyta forma, dar arčiau duomenų generavimo ar rinkimo vietos, taip pereinant nuo tradicinio modelio prie labai paskirstyto modelio (tinklo paribio kompiuterija);
- (18) duomenų centro paslaugų teikėjų siūlomos paslaugos ne visada gali būti teikiamos debesijos kompiuterijos paslaugos forma. Atitinkamai, duomenų centrai ne visada gali priklausyti debesijos kompiuterijos infrastruktūrai. Siekiant valdyti visą riziką, kuri kyla tinklų ir informacinių sistemų saugumui, ši direktyva taip pat turėtų būti taikoma tokių duomenų centrų paslaugoms, kurios nėra debesijos kompiuterijos paslaugos. Taikant šią direktyvą, sąvoka „duomenų centro paslauga“ turėtų apimti teikiamą paslaugą, kuri apima struktūras arba struktūrų grupes, skirtas informacinių technologijų ir tinklo įrangos centralizuotam pritaikymui, tarpusavio junglumui ir eksploatavimui, teikiant duomenų saugojimo, tvarkymo ir transportavimo paslaugas kartu su visa energijos paskirstymo ir aplinkos kontrolės įranga ir infrastruktūra. sąvoka „duomenų centro paslauga“ netaikoma vidaus, korporatyviniams duomenų centrams, kurie priklauso atitinkamam subjektui ir yra eksploatuojami to subjekto reikmėms;
- (19) pašto paslaugų teikėjams, kaip tai suprantama Europos Parlamento ir Tarybos direktyvoje 97/67/EB¹⁸, [...] **įskaitant** [...] kurjerių [...] paslaugų teikėjus, 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;

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).

- (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;
- (20a) aukšto kibernetinio saugumo lygio užtikrinimo ir išlaikymo tikslais pagal šią direktyvą reikalaujamas nacionalines kibernetinio saugumo strategijas turėtų sudaryti nuoseklios sistemos, kuriose būtų numatytas kibernetinio saugumo srities valdymas. Šias strategijas gali sudaryti vienas ar keli teisėkūros arba ne teisėkūros pobūdžio dokumentai;**
- (21) atsižvelgiant į nacionalinių valdymo struktūrų skirtumus ir siekiant išsaugoti jau veikiančias sektorių sistemas ar Sąjungos priežiūros ir reguliavimo įstaigas, valstybės narės turėtų turėti teisę paskirti daugiau nei vieną nacionalinę kompetentingą instituciją, atsakingą už užduočių, susijusių su esminių ir svarbių subjektų tinklų ir informacinių sistemų saugumu, vykdymą pagal šią direktyvą. Valstybės narės turėtų gebėti paskirti šį vaidmenį esamai institucijai;

- (22) siekiant palengvinti tarpvalstybinį institucijų bendradarbiavimą ir ryšių palaikymą bei sudaryti sąlygas veiksmingai įgyvendinti šią direktyvą, būtina, kad kiekviena valstybė narė paskirtų nacionalinį bendrąjį informacinį centrą, atsakingą už klausimų, susijusių su tinklų ir informacinių sistemų saugumu, koordinavimą ir tarpvalstybinį bendradarbiavimą Sąjungos lygmeniu;
- (23) kompetentingos institucijos arba CSIRT turėtų veiksmingai ir efektyviai iš subjektų gauti pranešimus apie incidentus, **taip pat siekiant, kai tinkama, palengvinti reagavimą į incidentus laiku ir pateikti atsakymą pranešančiajam subjektui**. Bendriesiems informaciniams centrams turėtų būti pavesta persiųsti pranešimus apie incidentus kitų paveiktų valstybių narių bendriesiems informaciniams centrams; [...]

- (23a) **konkreiems sektoriams taikomuose Sąjungos teisės aktuose, pagal kuriuos reikalaujama taikyti kibernetinio saugumo rizikos valdymo priemonės arba vykdyti pareigas pranešti, kurių poveikis yra bent lygiavertis šioje direktyvoje nustatytiems reikalavimams ir pareigoms, galėtų būti nustatyta, kad jų paskirtosios kompetentingos institucijos naudotųsi savo priežiūros ir vykdymo užtikrinimo įgaliojimais, susijusiais su tokiais priemonėmis arba pareigomis, padedant pagal šią direktyvą paskirtoms kompetentingoms institucijoms. Atitinkamos kompetentingos institucijos šiuo tikslu turėtų sudaryti bendradarbiavimo susitarimus. Tokiuose bendradarbiavimo susitarimuose, be kita ko, galėtų būti nustatytos priežiūros veiklos koordinavimo procedūros, įskaitant tyrimų ir patikrinimų vietoje procedūras laikantis nacionalinės teisės, ir kompetentingų institucijų keitimosi atitinkama informacija apie priežiūrą ir vykdymo užtikrinimą, įskaitant prieigą prie su kibernetine sritimi susijusios informacijos, kurios prašo pagal šią direktyvą paskirtos kompetentingos institucijos, mechanizmą;**
- (24) valstybės narės turėtų būti tinkamai pasirengusios – turėti tiek techninių, tiek organizacinių pajėgumų, kad galėtų išvengti su tinklų ir informacinėmis sistemomis susijusių incidentų bei rizikos, juos nustatyti, į juos reaguoti ir sušvelninti jų poveikį. Todėl valstybės narės turėtų užtikrinti, kad jose būtų gerai veikiančios CSIRT, dar vadinamos reagavimo į kompiuterių incidentus tarnybos, atitinkančios esminius reikalavimus, kad būtų garantuoti veiksmingi bei suderinami incidentų bei rizikos valdymo pajėgumai ir užtikrintas veiksmingas bendradarbiavimas Sąjungos lygmeniu. Atsižvelgiant į pasitikėjimu grindžiamų santykių tarp subjektų ir CSIRT stiprinimą, tais atvejais, kai CSIRT veikia kompetentingoje institucijoje, valstybės narės [...] **gali** svarstyti galimybę funkcinio požiūriu atskirti CSIRT vykdomas operatyvines užduotis, visų pirma susijusias su dalijimusi informacija ir parama subjektams, ir kompetentingų institucijų priežiūros veiklą;

- (25) kalbant apie asmens duomenis pažymėtina, kad CSIRT turėtų turėti galimybę pagal Europos Parlamento ir Tarybos Reglamentą (ES) 2016/679¹⁹ dėl asmens duomenų subjekto vardu ir jo prašymu pagal šią direktyvą imtis iniciatyvos patikrinti tinklų ir informacines sistemas, naudojamas jų paslaugoms teikti. **Kai taikytina**, valstybės narės turėtų siekti užtikrinti vienodą visų sektorių CSIRT techninių pajėgumų lygį. Valstybės narės gali paprašyti Europos Sąjungos kibernetinio saugumo agentūros (ENISA) padėti kurti nacionalines CSIRT;
- (26) atsižvelgiant į tarptautinio bendradarbiavimo kibernetinio saugumo srityje svarbą, CSIRT turėtų turėti galimybę dalyvauti ne tik šia direktyva sukurto CSIRT tinklo, bet ir tarptautinio bendradarbiavimo tinklų veikloje. **Todėl CSIRT ir kompetentingos institucijos galėtų keistis informacija, įskaitant asmens duomenis, su trečiųjų valstybių ar jų institucijų CSIRT, siekiant vykdyti jų užduotis pagal Reglamentą (ES) 2016/679. Tais atvejais, kai pagal Reglamento (ES) 2016/679 45 straipsnį nėra priimtas sprendimas dėl tinkamumo arba pagal to reglamento 46 straipsnį – dėl tinkamų apsaugos priemonių, keitimasis asmens duomenimis, kuris laikomas reikalingu siekiant sumažinti dideles kibernetines grėsmes ir reaguoti į vykstantį didelį incidentą, galėtų būti laikomas svarbia viešojo intereso priežastimi, kaip tai suprantama Reglamento (ES) 2016/679 49 straipsnio 1 dalies d punkte;**

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).

- (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;
- (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 **arba administruojantys** subjektai turėtų nustatyti atitinkamas procedūras, kurias taikant būtų šalinami aptikti pažeidžiamumai. Kadangi pažeidžiamumus dažnai aptinka ir apie juos praneša (atskleidžia) trečiosios šalys (pranešimus teikiantys 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 [...] **29147** pateikiamos gairės atitinkamai dėl pažeidžiamumų šalinimo ir atskleidimo. Kalbant apie pažeidžiamumų atskleidimą pažymėtina, kad ypač svarbus pranešimus teikiančių subjektų ir IRT produktų ar paslaugų gamintojų arba teikėjų koordinavimas. Suderintas pažeidžiamumų atskleidimas yra struktūrinis procesas, per kurį organizacijoms pranešama apie pažeidžiamumus taip, kad joms būtų sudarytos sąlygos problemą nustatyti ir išspręsti prieš atskleidžiant išsamią informaciją apie pažeidžiamumus trečiosioms šalims arba visuomenei. Suderintas pažeidžiamumų atskleidimas taip pat turėtų apimti pranešimus teikiančio subjekto ir organizacijos koordinavimą atsižvelgiant į taisymo laiką ir paskelbimą apie pažeidžiamumus;

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).

- (29) todėl valstybės narės turėtų imtis priemonių ir nustatyti atitinkamą nacionalinę politiką, kad palengvintų suderintą pažeidžiamumų atskleidimą. **Vykdydamos savo nacionalinę politiką, valstybės narės turėtų siekti kuo didesniu mastu reaguoti į iššūkius, su kuriais susiduria pažeidžiamumų tyrėjai, įskaitant jų galimą baudžiamosios atsakomybės riziką, laikantis jų nacionalinės teisinės sistemos.** [...] Valstybės narės turėtų paskirti CSIRT, kad jos imtųsi koordinatoriaus vaidmens ir prireikus veiktų kaip pranešimus teikiančių subjektų ir IRT produktų arba paslaugų gamintojų ar teikėjų tarpininkas. CSIRT koordinatoriaus užduotys visų pirma turėtų apimti atitinkamų subjektų nustatymą ir susisiekimą su jais, pranešimus teikiančių subjektų rėmimą, derybas dėl informacijos atskleidimo tvarkaraščių ir pažeidžiamumų, kurie daro poveikį kelioms organizacijoms, valdymą (kelių šalių **suderintas** pažeidžiamumų atskleidimas). Kai **praneštas** pažeidžiamumas **galėtų turėti didelį poveikį subjektams** [...] daugiau nei vienoje valstybėje narėje, **kai tikslinga**, paskirtosios CSIRT [...] turėtų bendradarbiauti CSIRT tinkle;
- (30) prieiga prie teisingos ir laiku pateikiamos informacijos apie pažeidžiamumus, kurie daro poveikį IRT produktams ir paslaugoms, padeda geriau valdyti kibernetinio saugumo riziką. Šiuo atžvilgiu viešai prieinamos informacijos apie pažeidžiamumus šaltiniai yra svarbi ne tik subjektų ir jų naudotojų, bet ir nacionalinių kompetentingų institucijų bei CSIRT priemonė. Dėl šios priežasties ENISA turėtų sukurti pažeidžiamumų registrą, kuriame esminiai ir svarbūs subjektai ir jų tiekėjai, taip pat subjektai, kurie nepatenka į šios direktyvos taikymo sritį, **arba paskirtosios CSIRT**, galėtų savanoriškai atskleisti pažeidžiamumus ir pateikti informaciją apie pažeidžiamumą, kuri sudarytų sąlygas naudotojams imtis atitinkamų rizikos mažinimo priemonių;

- (31) nors panašūs pažeidžiamųjų registrai arba duomenų bazės jau yra sukurti, jų prieglobą vykdo ir juos tvarko subjektai, kurie nėra įsisteigę Sąjungoje. ENISA tvarkomas pažeidžiamųjų registras padėtų užtikrinti didesnę paskelbimo proceso iki oficialaus pažeidžiamųjų 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 valstybių jurisdikcijose. **Visų pirma ENISA turėtų išnagrinėti galimybę glaudžiai bendradarbiauti su Bendros pažeidžiamųjų ir rizikos (BPR) sistemos operatoriais, įskaitant galimybę tapti šaknine BPR numeravimo institucija;**
- (32) **Bendradarbiavimo grupė turėtų toliau remti ir lengvinti valstybių narių strateginį bendradarbiavimą ir keitimąsi informacija, taip pat didinti jų pasitikėjimą ir patikimumą.** Bendradarbiavimo grupė turėtų kas dvejus metus parengti darbo programą, įskaitant veiksmus, kurių grupė turi imtis, kad pasiektų savo tikslus ir įvykdytų užduotis. Pirmosios pagal šią direktyvą priimtos programos laikotarpis turėtų būti suderintas su paskutinės programos, priimtos pagal Direktyvą (ES) 2016/1148, laikotarpiu, kad būtų išvengta galimų grupės darbo sutrikimų;
- (33) rengdama gairių dokumentus, Bendradarbiavimo grupė turėtų nuosekliai išsiaiškinti nacionalinius sprendimus ir patirtį, įvertinti Bendradarbiavimo grupės rezultatų poveikį nacionaliniam požiūriui, aptarti įgyvendinimo problemas ir suformuluoti konkrečias rekomendacijas, į kurias turėtų būti atsižvelgiama geriau įgyvendinant dabartines taisykles;

- (34) Bendradarbiavimo grupė turėtų išlikti lanksčiu forumu ir sugebėti reaguoti į kintančius ir naujus politikos prioritetus bei problemas ir kartu atsižvelgti į prieinamus išteklius. Ji turėtų nuolat rengti bendrus susitikimus su atitinkamais privačiais suinteresuotaisiais subjektais iš visos Sąjungos, kad aptartų grupės vykdomą veiklą ir surinktų informacijos apie naujus politikos uždavinius. Siekdama didinti bendradarbiavimą Sąjungos lygmeniu, grupė turėtų apsvarstyti galimybę pakviesti jos veikloje dalyvauti kibernetinio saugumo politiką įgyvendinančias Sąjungos įstaigas ir agentūras, pavyzdžiui, Europos kovos su elektroniniu nusikalstamumu centrą (EC3), Europos Sąjungos aviacijos saugos agentūrą (EASA) ir Europos Sąjungos kosmoso programos agentūrą (EUSPA);
- (35) kompetentingoms institucijoms ir CSIRT turėtų būti suteikti įgaliojimai dalyvauti pareigūnų iš kitų valstybių narių mainų programose siekiant pagerinti bendradarbiavimą. Kompetentingos institucijos turėtų imtis būtinų priemonių, kad pareigūnai iš kitų valstybių narių galėtų veiksmingai dalyvauti priimančiosios kompetentingos institucijos veikloje;
- (35a) CSIRT tinklas turėtų toliau padėti stiprinti valstybių narių pasitikėjimą bei patikimumą ir skatinti spartų ir efektyvų operatyvinį bendradarbiavimą. Siekdamas intensyvuoti operatyvinį bendradarbiavimą Sąjungos lygmeniu, CSIRT tinklas turėtų apsvarstyti galimybę pakviesti savo darbe dalyvauti kibernetinio saugumo politikos srityje veikiančias Sąjungos įstaigas ir agentūras, pavyzdžiui, Europolą;**
- (36) [...]

- (36a) siekdamos palengvinti šios direktyvos nuostatų, pavyzdžiui, dėl pažeidžiamumų valdymo, kibernetinio saugumo rizikos valdymo, pranešimo priemonių ir dalijimosi informacija tvarkos, veiksmingą įgyvendinimą, valstybės narės gali bendradarbiauti su trečiosiomis valstybėmis ir imtis veiklos, kuri laikoma tinkama tam tikslui, įskaitant keitimąsi informacija apie grėsmes, incidentus, pažeidžiamumus, priemones ir metodus, taktiką, metodiką ir procedūras, kibernetinių krizių valdymo parengtį ir pratybas, mokymus, pasitikėjimo stiprinimą ir struktūrizuoto dalijimosi informacija tvarką. Tokie bendradarbiavimo susitarimai turėtų atitikti Sąjungos teisę dėl duomenų apsaugos;
- (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, **kad būtų išvengta užduočių dubliavimosi**. 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 **politiniu** 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;

- (37a) **didelio masto kibernetinio saugumo incidentų ir krizių atvejais EU-CyCLONe turėtų veikti kaip techninio ir politinio lygmens tarpinis tinklas. Jis turėtų stiprinti bendradarbiavimą operatyviniu lygmeniu, remdamasis CSIRT tinklo išvadomis ir naudodamas savo pajėgumus, kad būtų rengiamos didelio poveikio incidentų ir krizių poveikio analizės ir remiamas sprendimų priėmimas politiniu lygmeniu. ES institucijos, įstaigos ir agentūros turėtų paskirti už didelio masto saugumo incidentų ir krizių valdymą atsakingą kompetentingą instituciją, kuri taptų EU-CyCLONe nare;**
- (38) [...]
- (39) [...]
- (39a) **atsakomybė už tinklų ir informacinių sistemų saugumo užtikrinimą didžia dalimi tenka esminiams ir svarbiems subjektams. Turėtų būti skatinama ir plėtojama rizikos valdymo kultūra, apimanti rizikos vertinimą ir esamą riziką atitinkančių saugumo priemonių įgyvendinimą;**
- (40) **rizikos valdymo priemonėse turėtų būti atsižvelgiama į subjekto priklausomybę nuo tinklų ir informacinių sistemų ir jos 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;**

- (40a) kadangi grėsmė tinklų ir informacinių sistemų saugumui gali būti įvairios kilmės, šioje direktyvoje laikomasi visų rūšių pavojus apimančio požiūrio, kuris apima tinklų ir informacinių sistemų bei jų fizinės aplinkos apsaugą nuo visų tokių įvykių kaip vagystė, gaisras, potvynis, telekomunikacijų ar elektros energijos tiekimo triktys, arba nuo neleistinos fizinės prieigos prie subjekto informacijos ir informacijos tvarkymo objektų ir žalos jiems ar jų trikdžių, kurie galėtų kelti pavojų saugomų, perduodamų ar tvarkomų duomenų arba teikiamų, per tinklus ir informacines sistemas prieinamų paslaugų prieinamumui, autentiškumui, vientisumui ar konfidencialumui. Todėl rizikos valdymo priemonėmis taip pat turėtų būti užtikrinamas fizinis ir aplinkos saugumas, įtraukiant priemones, skirtas tinklų ir informacinių sistemų apsaugai nuo sistemos gedimų, žmogaus klaidų, piktavališkų veiksmų ar gamtos reiškinių pagal Europos arba tarptautiniu mastu pripažintus standartus, pavyzdžiui, įtrauktus į ISO 27000 seriją. Šiuo atžvilgiu subjektai savo rizikos valdymo priemonėmis turėtų taip pat užtikrinti žmogiškųjų išteklių saugumą ir įdiegti tinkamą prieigos kontrolės politiką. Šios priemonės turėtų derėti su Direktyva XXXX [CER direktyva];**
- (40b) jei nėra pagal Reglamentą (ES) 2019/881 priimtų tinkamų Europos kibernetinio saugumo sertifikavimo schemų, valstybės narės galėtų reikalauti, kad subjektai naudotų sertifikuotus IRT produktus, paslaugas ir procesus arba gautų sertifikatą pagal esamas nacionalines kibernetinio saugumo schemas, kad būtų laikomasi pagal šią direktyvą nustatytą kibernetinio saugumo rizikos valdymo reikalavimų;**

- (41) siekiant neužkrauti neproporcingos finansinės ir administracinės naštos esminiams ir svarbiems subjektams, kibernetinio saugumo rizikos valdymo reikalavimai turėtų būti proporcingi rizikai, [...] kylančiai atitinkamai tinklų ir informacinei sistemai, atsižvelgiant į tokių priemonių modernumą **ir jų įgyvendinimo sąnaudas. Be to, turėtų būti tinkamai atsižvelgiama į subjekto dydį, taip pat incidentų tikimybę ir jų sunkumą;**
- (41a) **siekiant sumažinti reguliavimo naštą, kibernetinio saugumo rizikos valdymo priemonių įgyvendinimo reikalavimai, taikomi vidutiniams, mažiesiems ir labai mažiems subjektams, iš esmės turėtų būti švelnesni, nebent ypatingos svarbos kriterijai arba nacionaliniai rizikos vertinimai pateisintų griežtesnius reikalavimus, ypač subjektų, kurie atitinka šioje direktyvoje nustatytus su ypatinga svarba susijusius kriterijus, atžvilgiu;**
- (42) esminiai ir svarbūs subjektai turėtų užtikrinti tinklų ir informacinių sistemų, kurias jie naudoja savo veikloje, saugumą. Tai visų pirma būtų privačios tinklų ir informacinės sistemos, kurias administruoja jų vidaus IT personalas arba kurių saugumas užtikrinamas veiklos ranga. Kibernetinio saugumo rizikos valdymo ir pranešimų teikimo reikalavimai pagal šią direktyvą turėtų būti taikomi atitinkamiems esminiams ir svarbiems subjektams, nepaisant to, ar jų tinklų ir informacinių sistemų techninę priežiūrą vykdo vidaus darbuotojai, ar rangovai;
- (42aa) **atsižvelgiant į DNS paslaugų teikėjų, aukščiausio lygio domenų (TLD) vardų registru ir TLD atveju domenų vardų registravimo paslaugas teikiančių subjektų, debesijos kompiuterijos paslaugų teikėjų, duomenų centrų paslaugų teikėjų, turinio teikimo tinklo paslaugų teikėjų, valdomų paslaugų teikėjų ir valdomų saugumo paslaugų teikėjų tarpvalstybinį pobūdį, jiems turėtų būti taikomas didesnio lygio suderinimas Sąjungos lygmeniu. Todėl kibernetinio saugumo priemonių įgyvendinimas turėtų būti palengvintas įgyvendinimo aktu;**

- (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 piktaivališki dalyviai galėjo pažeisti subjekto tinklą ir informacinių sistemų saugumą pasinaudodami pažeidžiamumais, taip darydami poveikį trečiųjų šalių produktams ir paslaugoms. Todėl subjektai turėtų įvertinti ir atsižvelgti į bendrą savo tiekėjų ir paslaugų teikėjų produktų ir kibernetinio saugumo praktikos, įskaitant jų saugaus tobulinimo procedūras, kokybę;
- (44) kalbant apie paslaugų teikėjus pažymėtina, kad valdomų saugumo paslaugų teikėjai (MSSP) tokiose srityse kaip reagavimas į incidentus, skverbimosi testavimas, saugumo auditai ir konsultacijos atlieka itin svarbų vaidmenį padėdami subjektams atskleisti incidentus ir į juos reaguoti. Tačiau tie MSSP taip pat buvo pačių kibernetinių išpuolių taikiniai, o juos glaudžiai integravus į operatorių veiklą kyla tam tikra kibernetinio saugumo rizika. Todėl subjektai, atrinkdami MSSP, turėtų veikti atidžiau;
- (44a) nacionalinėms kompetentingoms institucijoms vykdant jų priežiūros užduotis taip pat gali būti naudingos kibernetinio saugumo paslaugos, pavyzdžiui, saugumo auditai ir skverbimosi testavimas arba reagavimas į incidentus. Siekiant padėti subjektams, taip pat nacionalinėms kompetentingoms institucijoms, pasirinkti kvalifikuotus ir patikimus kibernetinio saugumo paslaugų teikėjus, Komisija, padedama Bendradarbiavimo grupės ir ENISA, turėtų apsvarstyti galimybę pagal Reglamento (ES) 2018/881 48 straipsnį prašyti parengti Europos kibernetinio saugumo sertifikavimo schemas;**

- (45) subjektai taip pat turėtų mažinti kibernetinio saugumo riziką, kylančią dėl jų sąveikos ir santykių su kitais suinteresuotaisiais subjektais platesnėje ekosistemoje. Visų pirma subjektai turėtų imtis tinkamų priemonių siekdami užtikrinti, kad jų bendradarbiavimas su akademinėmis ir mokslinių tyrimų įstaigomis būtų vykdomas laikantis jų kibernetinio saugumo politikos ir būtų laikomasi gerosios praktikos, susijusios su saugia prieiga prie informacijos ir jos sklaida apskritai ir ypač su intelektinės nuosavybės apsauga. Be to, atsižvelgiant į duomenų svarbą ir vertę subjektų veiklai, kai jie priklauso nuo duomenų transformavimo ir duomenų analizės paslaugų, kurias teikia trečiosios šalys, subjektai turėtų imtis visų tinkamų kibernetinio saugumo priemonių;
- (46) siekiant toliau mažinti pagrindinę tiekimo grandinės riziką ir padėti subjektams, veikiantiems sektoriuose, kuriems taikoma ši direktyva, tinkamai valdyti su tiekimo grandine ir tiekėjais susijusią kibernetinio saugumo riziką, Bendradarbiavimo grupė, kurioje dalyvauja atitinkamos nacionalinės institucijos, bendradarbiaudama su Komisija ir ENISA, turėtų atlikti suderintus sektorių tiekimo grandinės rizikos vertinimus, kaip jau buvo padaryta 5G tinklų atveju pagal Rekomendaciją (ES) 2019/534 dėl 5G tinklų kibernetinio saugumo²¹, 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).

- (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) kokių mastu esminiai ir svarbūs subjektai naudojami konkrečiomis ypatingos svarbos IRT paslaugomis, sistemomis ar produktais ir nuo jų priklauso; ii) konkrečių ypatingos svarbos IRT paslaugų, sistemų ar produktų svarbą vykdant ypatingos svarbos arba neskelbtinas funkcijas, įskaitant asmens duomenų tvarkymą; iii) alternatyvių IRT paslaugų, sistemų ar produktų prieinamumą; iv) visos IRT paslaugų, sistemų ar produktų tiekimo grandinės atsparumą sutrikimams ir v) atsirandančių IRT paslaugų, sistemų ar produktų atveju, jų galimą būsimą svarbą subjektų veiklai;
- (48) siekiant supaprastinti viešųjų elektroninių ryšių tinklų ar viešai prieinamų elektroninių ryšių paslaugų teikėjams ir patikimumo užtikrinimo paslaugų teikėjams taikomas teisinės pareigas, susijusias su jų tinklų ir informacinių sistemų saugumu, taip pat sudaryti sąlygas tiems subjektams ir jų atitinkamoms kompetentingoms institucijoms pasinaudoti šioje direktyvoje nustatyta teisine sistema (įskaitant CSIRT, atsakingą už rizikos ir incidentų valdymą, kompetentingų institucijų ir įstaigų dalyvavimą Bendradarbiavimo grupės ir CSIRT tinklo veikloje, paskyrimą), jie turėtų būti įtraukti į šios direktyvos taikymo sritį. Todėl atitinkamos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014²² ir Europos Parlamento ir Tarybos direktyvos (ES) 2018/1972²³ nuostatos, susijusios su saugumo ir pranešimo reikalavimų nustatymu tų rūšių subjektams, turėtų būti panaikintos;

²² 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB (OL L 257, 2014 8 28, p. 73).

²³ 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas (OL L 321, 2018 12 17, p. 36).

- (48a) šioje direktyvoje nustatytos saugumo pareigos turėtų būti laikomos papildančiomis Reglamentu (ES) Nr. 910/2014 (eIDAS reglamentas) patikimumo užtikrinimo paslaugų teikėjams nustatytus reikalavimus. Patikimumo užtikrinimo paslaugų teikėjų turėtų būti prašoma imtis visų tinkamų ir proporcingų jų paslaugoms kylančios rizikos valdymo priemonių, be kita ko, klientų ir pasikliaujančiųjų trečiųjų šalių atžvilgiu, ir pagal šią direktyvą pranešti apie saugumo incidentus. Tokios saugumo ir pranešimo pareigos turėtų būti taikomos ir teikiamos paslaugos fizinei apsaugai. Toliau taikomas Reglamento (ES) Nr. 910/2014 24 straipsnis;
- (48aa) valstybės narės gali pavesti eIDAS priežiūros įstaigoms atlikti patikimumo užtikrinimo paslaugų srities kompetentingų institucijų vaidmenį, kad būtų užtikrintas dabartinės praktikos tęstinumas ir toliau plėtojamos taikant eIDAS reglamentą įgytos žinios ir patirtis. Kai tas vaidmuo pavedamas kitai įstaigai, pagal šią direktyvą kompetentingos institucijos turėtų glaudžiai ir laiku bendradarbiauti keisdamosi atitinkama informacija, kad būtų užtikrinta veiksminga patikimumo užtikrinimo paslaugų teikėjų priežiūra ir užtikrinta, kad jie laikytųsi šioje direktyvoje bei Reglamente [XXXX/XXXX] nustatytų reikalavimų.

Kai taikytina, pagal šią direktyvą kompetentinga nacionalinė institucija turėtų nedelsdama informuoti eIDAS priežiūros įstaigą apie visas dideles kibernetines grėsmes arba incidentus, darančius poveikį patikimumo užtikrinimo paslaugoms, apie kuriuos pranešta, taip pat apie visus atvejus, kai patikimumo užtikrinimo paslaugų teikėjai nesilaiko šioje direktyvoje nustatytų reikalavimų. Pranešimų teikimo tikslais valstybės narės, kai taikytina, gali naudotis viena bendra prieiga, nustatyta siekiant užtikrinti bendrą automatinį pranešimą apie incidentus tiek eIDAS priežiūros įstaigai, tiek pagal šią direktyvą kompetentingai institucijai. Taisyklės dėl pareigų pranešti neturėtų daryti poveikio Reglamentui (ES) 2016/679 ir Europos Parlamento ir Tarybos direktyvai 2002/58/EB²⁴;

²⁴ 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 37).

- (49) kai tinkama, siekiant išvengti nereikalingo trikdymo, **valstybių narių įgyvendinamomis šios direktyvos perkėlimo į nacionalinę teisę priemonėmis turėtų būti atsižvelgiama į esamas nacionalines gaires[...], priimtas siekiant į nacionalinę teisę perkelti taisykles, susijusias su Direktyvos (ES) 2018/1722 40[...] ir 41 straipsniuose nustatytomis saugumo priemonėmis[...], tokiu būdu plėtojant pagal Direktyvą (ES) 2018/1722 jau įgytas žinias ir įgūdžius, susijusias su saugumo rizikos valdymo priemonėmis ir pranešimais apie incidentus. ENISA taip pat gali parengti gaires dėl saugumo ir pranešimų teikimo reikalavimų, skirtas viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjams, kad būtų sudarytos palankesnės sąlygos suderinimui bei pertvarkai ir kuo labiau sumažinti trikdžiai. Valstybės narės gali pavesti nacionalinėms reguliavimo institucijoms atlikti elektroninių ryšių srities kompetentingų institucijų vaidmenį, kad būtų užtikrintas dabartinės praktikos tęstinumas ir toliau plėtojamos taikant Direktyvą (ES) 2018/1722 įgytos žinios ir patirtis;**
- (50) atsižvelgiant į didėjančią su numeriu nesiejamo asmenų tarpusavio ryšio paslaugų svarbą, būtina užtikrinti, kad tokioms paslaugoms, atsižvelgiant į jų specifinį pobūdį ir ekonominę svarbą, taip pat būtų taikomi tinkami saugumo reikalavimai. Todėl tokių paslaugų teikėjai taip pat turėtų užtikrinti tinklų ir informacinių sistemų saugumo lygį, atitinkantį keliamą riziką. Atsižvelgiant į tai, kad su numeriu nesiejamo asmenų tarpusavio ryšio paslaugų teikėjai paprastai neturi tikrų galimybių valdyti tinklais siunčiamus perdavimo signalus, galima laikyti, kad tam tikrais atžvilgiais tokioms paslaugoms kyla mažesnio laipsnio rizika nei tradicinėms elektroninių ryšių paslaugoms. Tas pats pasakytina ir apie asmenų tarpusavio ryšio paslaugas, kurias teikiant naudojami numeriai ir kurias teikiant faktiškai nekontroliuojamas signalų perdavimas;

- (51) vidaus rinka labiau nei kada nors anksčiau priklauso nuo interneto veikimo. Beveik visų esminių ir svarbių subjektų paslaugos priklauso nuo internetu teikiamų paslaugų. Siekiant užtikrinti sklandų esminių ir svarbių subjektų teikiamų paslaugų teikimą, svarbu, kad viešuosiuose elektroninių ryšių tinkluose, pavyzdžiui, interneto magistralėse ar povandeniniuose ryšių kabeliuose, būtų įdiegtos tinkamos kibernetinio saugumo priemonės ir būtų pranešama apie su jomis susijusius incidentus;
- (52) kai [...] **taikytina**, subjektai turėtų informuoti savo paslaugų gavėjus apie konkrečias [...] priemones, kurių jie gali imtis, kad sumažintų jiems **dėl didelės kibernetinės grėsmės** kylančią riziką. **Kai tinkama, visų pirma tais atvejais, kai didelė kibernetinė grėsmė gali tapti realia, apie tai pranešdami kompetentingoms institucijoms arba CSIRT, subjektai turėtų apie pačią grėsmę pranešti ir savo paslaugų gavėjams.** 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 **kibernetines** [...] grėsmes gavėjams turėtų būti teikiama nemokamai;
- (53) visų pirma viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai turėtų informuoti paslaugų gavėjus apie konkrečias ir dideles kibernetines grėsmes ir priemones, kurių jie gali imtis savo ryšių saugumui užtikrinti, pavyzdžiui, naudodami konkrečių rūšių programinę įrangą arba šifravimo technologijas;

- (54) siekiant užtikrinti elektroninių ryšių tinklų ir paslaugų saugumą, turėtų būti skatinama naudoti šifravimą, visų pirma ištininį 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. Ištininio 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 ištininiuose šifruotuose ryšiuose, turėtų išlaikyti šifravimo veiksmingumą apsaugant ryšių privatumą ir saugumą, kartu užtikrinant veiksmingą atsaką į nusikalstamumą;
- (55) šia direktyva nustatomas dviejų etapų pranešimų apie incidentus teikimo metodas, siekiant užtikrinti tinkamą pusiausvyrą tarp, viena vertus, greito pranešimų teikimo, kuris padeda sumažinti galimą incidentų plitimą ir suteikia galimybę subjektams prašyti paramos, ir, kita vertus, išsamių pranešimų, kuriuose atsižvelgiama į vertingą su pavieniais incidentais susijusią patirtį ir ilginiui 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 išteklių nebūtų nukreipti nuo veiklos, susijusios su incidentų valdymu, kuriam turėtų būti teikiama pirmenybė. Siekdamos toliau užkirsti kelią tam, kad vykdant pareigas pranešti apie incidentus išteklių 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;

- (55a) **proaktyvus požiūris į kibernetines grėsmes yra gyvybiškai svarbus kibernetinio saugumo rizikos valdymo elementas, kuris turėtų sudaryti sąlygas kompetentingoms institucijoms veiksmingai užkirsti kelią kibernetinių grėsmių tapimui faktiniais incidentais, dėl kurių gali būti patiriama didelių materialinių ar nematerialinių nuostolių. Tuo tikslu labai svarbu, kad apie dideles kibernetines grėsmes būtų pranešama;**
- (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 sukuriamą papildomą našta ir gali kilti neaiškumų dėl tokių pranešimų formos ir procedūrų. Atsižvelgiant į tai ir siekiant supaprastinti pranešimų apie saugumo incidentus teikimą, valstybės narės [...] **galėtų** sukurti *vieną bendrą prieigą* visiems pranešimams, kuriuos reikalaujama pateikti pagal šią direktyvą ir kitus Sąjungos teisės aktus, pavyzdžiui, Reglamentą (ES) 2016/679 ir Direktyvą 2002/58/EB. ENISA, bendradarbiaudama su Bendradarbiavimo grupe, turėtų parengti bendrus pranešimo šablonus, pateikdama gaires, kuriomis būtų supaprastinta ir racionalizuota pagal Sąjungos teisę reikalaujama pranešimų teikimo informacija ir sumažinta bendrovėms tenkanti našta;
- (57) kai įtariama, kad incidentas yra susijęs su sunkia nusikalstama veika pagal Sąjungos arba nacionalinę teisę, valstybės narės turėtų skatinti esminius ir svarbius subjektus, remiantis Sąjungos teisę atitinkančiomis taikytinomis baudžiamojo proceso taisyklėmis, pranešti atitinkamoms teisėsaugos institucijoms apie įtariamus sunkius nusikalstamo pobūdžio incidentus. Atitinkamais atvejais ir nepažeidžiant Europolui taikomų asmens duomenų apsaugos taisyklių, pageidautina, kad skirtingų valstybių narių kompetentingų institucijų ir teisėsaugos institucijų veiklos koordinavimą palengvintų EC3 ir ENISA;

- (58) daugeliu atvejų dėl incidentų kyla pavojus asmens duomenų saugumui. Tokiomis aplinkybėmis kompetentingos institucijos turėtų bendradarbiauti ir keistis informacija visais svarbiais klausimais su duomenų apsaugos institucijomis ir priežiūros institucijomis pagal Direktyvą 2002/58/EB;
- (59) siekiant užtikrinti DNS saugumą, stabilumą ir atsparumą, būtina turėti tikslias ir išsamias domenų vardų ir registracijos duomenų (vadinamųjų WHOIS duomenų) bazes ir suteikti teisėtą prieigą prie tokių duomenų, o tai savo ruožtu prisideda prie aukšto bendro kibernetinio saugumo lygio Sąjungoje. Kai tvarkomi asmens duomenys, toks tvarkymas turi atitikti Sąjungos duomenų apsaugos teisės aktus;
- (60) šių duomenų prieinamumas ir galimybė laiku su jais susipažinti valdžios institucijoms, įskaitant kompetentingas institucijas pagal Sąjungos ar nacionalinę teisę nusikalstamų veikų prevencijos, tyrimo ar baudžiamojo persekiojimo už jas tikslais, CERT, CSIRT ir elektroninių ryšių tinklų ir paslaugų teikėjams ir tų klientų vardu veikiančių kibernetinio saugumo technologijų ir paslaugų teikėjams tiek, kiek tai susiję su jų klientų duomenimis, yra labai svarbūs siekiant užkirsti kelią piktnaudžiavimui domenų vardų sistema ir su juo kovoti, visų pirma siekiant užkirsti kelią kibernetinio saugumo incidentams, juos aptikti ir į juos reaguoti. Tokia prieiga turėtų atitikti Sąjungos duomenų apsaugos teisę tiek, kiek ji susijusi su asmens duomenimis;
- (61) siekiant užtikrinti tikslių ir išsamių domenų vardų registracijos duomenų prieinamumą, aukščiausio lygio domenų vardų registrai ir aukščiausio lygio domenų atveju domenų vardų registravimo paslaugas teikiantys subjektai (vadinamieji registratoriai), turėtų rinkti domenų vardų registracijos duomenis ir užtikrinti jų vientisumą ir prieinamumą. **Registracijos duomenų atveju subjektai turėtų visų pirma patikrinti registruotojo vardą ir pavardę (pavadinimą) ir e. pašto adresą.** [...] Aukščiausio lygio domenų vardų registrai ir aukščiausio lygio domenų atveju domenų vardų registravimo paslaugas teikiantys subjektai turėtų nustatyti politiką ir procedūras, skirtas tikslams ir išsamiems registracijos duomenims rinkti ir saugoti, taip pat užkirsti kelią netikslams registracijos duomenims ir juos ištaisyti pagal Sąjungos duomenų apsaugos taisykles;

- (62) aukščiausio lygio domenų vardų registrai ir jiems skirtas domenų vardų registravimo paslaugas teikiantys subjektai turėtų viešai skelbti domenų vardų registracijos duomenis, kuriems netaikomos Sąjungos duomenų apsaugos taisyklės, pavyzdžiui, duomenis, susijusius su juridiniais asmenimis²⁵. 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 [...] **teisėtai prieigos siekiančių subjektų, pavyzdžiui, pagal Sąjungos arba nacionalinę teisę nacionalinio saugumo ir baudžiamosios justicijos srityse kompetentingų institucijų arba CSIRT, 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. **Valstybės narės turėtų užtikrinti, kad visų rūšių prieiga prie domenų registracijos duomenų (tiek asmens, tiek ne asmens duomenų) būtų nemokama.** Siekdama skatinti suderintą praktiką visoje vidaus rinkoje, Komisija gali priimti tokių procedūrų gaires, nepažeisdama Europos duomenų apsaugos valdybos kompetencijos, **atsižvelgdama į įvairių suinteresuotųjų subjektų bendruomenės parengtus tarptautinius standartus ir juos papildydama;**

²⁵ 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“.

- (63) [...] esminiai ir svarbūs subjektai, kuriems taikoma ši direktyva, turėtų priklausyti valstybės narės, kurioje jie teikia savo paslaugas, jurisdikcijai. **Šios direktyvos I priedo 1–7 ir 10 punktuose nurodyti subjektai, I priedo 8 punkte nurodyti patikimumo užtikrinimo paslaugų teikėjai ir interneto duomenų srautų mainų taško teikėjai ir II priedo 1–5 punktuose nurodyti subjektai turėtų priklausyti valstybės narės, kurioje jie yra įsisteigę, jurisdikcijai.** Jeigu subjektas teikia paslaugas arba turi padalinių 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. **Kai valstybės narės nusprendžia vykdyti jurisdikciją, jos turėtų vengti, kad už šioje direktyvoje nustatytų pareigų pažeidimą būtų baudžiama daugiau nei vieną kartą;**
- (64) siekiant atsižvelgti į DNS paslaugų teikėjų, aukščiausio lygio domenų vardų registru, **aukščiausio lygio domenų vardų atveju domenų vardų registravimo paslaugas teikiančių subjektų,** 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 nuolatinės 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 **daugiausia** priimami su kibernetinio saugumo rizikos valdymo priemonėmis susiję sprendimai. Paprastai ji sutampa su įmonių centrinės administracijos vieta Sąjungoje. Jei **vieta, kurioje tokie sprendimai daugiausia priimami, negali būti nustatyta, arba** 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;

- (64a) **kai viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjas teikia rekursinę DNS paslaugą tik kaip interneto prieigos paslaugos dalį, subjektas turi būti laikomas priklausančiu visų valstybių narių, kuriose teikiamos jo paslaugos, jurisdikcijai;**
- (64aa) **siekiant užsitikrinti aiškų vaizdą apie DNS paslaugų teikėjus, aukščiausio lygio domeno vardų registrus, aukščiausio lygio domenų vardų atveju domenų vardų registravimo paslaugas teikiančius subjektus, turinio teikimo tinklo paslaugų teikėjus, debesijos kompiuterijos paslaugų teikėjus, duomenų centro paslaugų teikėjus ir skaitmeninių paslaugų teikėjus, teikiančius paslaugas visoje Sąjungoje šios direktyvos taikymo srityje, ENISA turėtų sukurti ir tvarkyti tokių subjektų registrą, grindžiamą iš valstybių narių gautais pranešimais, kai taikytina, teikiamais pagal jų nacionalinius pranešimo apie save mechanizmus. Kad būtų užtikrintas į šį registrą įtrauktinos informacijos tikslumas ir išsamumas, valstybės narės turėtų pateikti ENISA jų nacionaliniuose registruose turimą informaciją apie tuos subjektus. ENISA ir valstybės narės turėtų imtis priemonių tokių registrų sąveikumui palengvinti, kartu užtikrindamos konfidencialios ar įslaptintos informacijos apsaugą;**

- (65) tais atvejais, kai paslaugas Sąjungoje siūlo DNS paslaugų teikėjas, aukščiausio lygio domenų vardų registras, turinio teikimo tinklo paslaugų teikėjas, debesijos kompiuterijos paslaugų teikėjas, duomenų centro paslaugų teikėjas ir skaitmeninių paslaugų teikėjas, kurie nėra įsisteigę Sąjungoje, tokie tiekėjai turėtų paskirti atstovą. Siekiant nustatyti, ar toks subjektas siūlo paslaugas Sąjungoje, reikėtų įvertinti, ar akivaizdu, kad subjektas ketina siūlyti paslaugas asmenims vienoje ar keliose valstybėse narėse. Vien to, kad Sąjungoje prieinama subjekto ar tarpininko interneto svetainė arba e. pašto adresas ir kiti kontaktiniai duomenys arba kad vartojama kalba, kuri paprastai vartojama trečiojoje valstybėje, kurioje yra įsisteigęs subjektas, nepakanka siekiant įrodyti, kad esama tokio ketinimo. Tačiau dėl tokių veiksmų kaip kalba ar valiuta, paprastai vartojamų (naudojamų) vienoje ar daugiau valstybių narių, įskaitant galimybę užsakyti paslaugas ta kita kalba, arba nurodant Sąjungoje esančius vartotojus ar naudotojus, gali būti akivaizdu, kad subjektas ketina siūlyti paslaugas Sąjungoje. Atstovas turėtų veikti subjekto vardu, o kompetentingos institucijos arba CSIRT turėtų turėti galimybę kreiptis į atstovą. Atstovas turėtų būti aiškiai paskirtas rašytiniu subjekto įgaliojimu veikti pastarojo vardu vykdant jo pareigas pagal šią direktyvą, įskaitant pranešimą apie incidentus;

- (66) jeigu pagal šios direktyvos nuostatas keičiamasi informacija, kuri laikoma įslaptinta pagal nacionalinę arba Sąjungos teisę, apie ją pranešama arba ja kitaip dalijamasi, turėtų būti taikomos atitinkamos konkrečios įslaptintos informacijos tvarkymo taisyklės;
- (67) kadangi kibernetinės grėsmės tampa vis sudėtingesnės ir painesnės, geros aptikimo ir prevencijos priemonės labai priklauso nuo to, ar subjektai reguliariai keičiasi žvalgybos informacija apie grėsmes ir pažeidžiamumą. Dalijantis informacija padedama didinti informuotumą apie kibernetines grėsmes, o tai savo ruožtu didina subjektų gebėjimą užkirsti kelią grėsmėms virsti tikrais incidentais ir sudaro sąlygas subjektams geriau suvaldyti incidentų poveikį ir veiksmingiau atkurti veiklą. Nesant gairių Sąjungos lygmeniu, atrodo, kad keli veiksniai trukdo dalytis žvalgybos informacija, visų pirma netikrumas dėl suderinamumo su konkurencijos ir atsakomybės taisyklėmis;
- (68) subjektai turėtų būti skatinami bendrai naudotis savo asmeninėmis žiniomis ir praktine patirtimi strateginiu, taktiniu ir veiklos lygmenimis, kad sustiprintų savo gebėjimus tinkamai vertinti, stebėti kibernetines grėsmes, apsaugoti nuo jų ir į jas reaguoti. Todėl būtina sudaryti sąlygas Sąjungos lygmeniu kurti savanoriško keitimosi informacija mechanizmus. Šiuo tikslu valstybės narės turėtų aktyviai remti ir skatinti atitinkamus subjektus, kuriems netaikoma ši direktyva, dalyvauti tokiuose keitimosi informacija mechanizmuose. Tie mechanizmai turėtų būti taikomi visapusiškai laikantis Sąjungos konkurencijos taisyklių ir Sąjungos teisės nuostatų dėl duomenų apsaugos;

- (69) **esminių ir svarbių** subjektų [...] ir saugumo technologijų bei paslaugų teikėjų **vykdomas asmens duomenų tvarkymas** tokiu mastu, koku tai tikrai būtina ir proporcinga tinklų ir informacijos saugumo užtikrinimo tikslais, **galėtų būti laikomas būtinu, kad būtų įvykdyta teisinė prievolė, arba [...]** būti teisėtas atitinkamo duomenų valdytojo interesas[...], kaip nurodyta Reglamente (ES) 2016/679. Tai **galėtų [...]** apimti priemonės, susijusias su incidentų prevencija, aptikimu, analize ir reagavimu į juos, informuotumo apie konkrečias kibernetines grėsmes didinimo priemonės, 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 priemonės. Taikant tokias priemones gali prireikti tvarkyti [...] **įvairių** rūšių asmens duomenis, **pavyzdžiui:** IP adresus, universaliuosius išteklių adresus (URL), domenų vardus ir e. pašto adresus. **Nacionalinėje teisėje turėtų būti nustatyta, kad kompetentingos institucijos, bendrieji informaciniai punktai ir CSIRT tvarko asmens duomenis ir toks duomenų tvarkymas turėtų būti laikomas būtinu, kad būtų įvykdyta teisinė prievolė, arba siekiant įvykdyti užduotį, vykdomą viešojo intereso labui, arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas, kaip nurodyta Reglamento (ES) 2016/679 6 straipsnio 1 dalies c arba e punkte;**
- (69a) valstybių narių įstatymais gali būti nustatytos taisyklės, kuriomis kompetentingoms institucijoms, bendriesiems informaciniams punktams ir CSIRT būtų leidžiama tokiu mastu, koku tai tikrai būtina ir proporcinga esminių ir svarbių subjektų tinklų ir informacinių sistemų saugumo užtikrinimo tikslais, tvarkyti specialių kategorijų asmens duomenis pagal Reglamento (ES) 2016/679 9[...] straipsnį, visų pirma numatant tinkamas ir konkrečias fizinių asmenų pagrindinių teisių ir interesų apsaugos priemones, įskaitant pakartotinio tokių duomenų naudojimo techninius apribojimus ir galimybę naudoti pažangiąsias saugumo ir privatumo apsaugos priemones, pavyzdžiui, pseudoniminimą, arba, jei anoniminimas reikšmingai paveiktų tikslą, kurio siekiama – šifravimą;

- (70) siekiant sustiprinti priežiūros įgaliojimus ir veiksmus, padedančius užtikrinti veiksmingą reikalavimų laikymąsi, šioje direktyvoje turėtų būti nustatytas būtiniausias priežiūros veiksmų ir priemonių, kuriomis kompetentingos institucijos **galėtų** [...] prižiūrėti esminius ir svarbius subjektus, sąrašas. Be to, šioje direktyvoje turėtų būti nustatyta atskira esminių ir svarbių subjektų priežiūros tvarka, siekiant užtikrinti teisingą tiek subjektų, tiek kompetentingų institucijų pareigų pusiausvyrą. Taigi esminiams subjektams turėtų būti taikoma visavertė priežiūros tvarka (*ex ante* ir *ex post*), o svarbiems subjektams turėtų būti taikoma negriežta priežiūros tvarka, t. y. tik *ex post*. Pastaruoju atveju tai reiškia, kad iš svarbių subjektų neturėtų **būti reikalaujama** [...] 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. **Svarbių subjektų atveju *ex post* priežiūra gali būti pradėta remiantis kompetentingoms institucijoms pateiktais įrodymais arba požymiais ar informacija, kurie, šių institucijų manymu, rodo, kad gali būti nesilaikoma šioje direktyvoje nustatytų pareigų. Pavyzdžiui, tai galėtų būti tokios pačios rūšies įrodymai, požymiai ar informacija, kuriuos kompetentingai institucijai pateikia kitos institucijos, subjektai, piliečiai, žiniasklaida ar kiti šaltiniai, viešai prieinama informacija arba informacija, kurią kompetentingos institucijos gali gauti vykdydamos kitą jų užduotims atlikti reikalingą veiklą;**

- (70a) vykdydamos *ex ante* priežiūrą, kompetentingos institucijos turėtų galėti proporcingai nuspręsti dėl priežiūros veiksmų ir jų turimų priemonių naudojimo prioritetų nustatymo. Tai reiškia, kad kompetentingos institucijos gali nuspręsti dėl tokių prioritetų nustatymo remdamosi priežiūros metodikomis, pagal kurias turėtų būti laikomasi rizika grindžiamo požiūrio. Konkrečiau, tokios metodikos galėtų apimti esminių subjektų klasifikavimo pagal rizikos kategorijas kriterijus ar lyginamuosius standartus, atitinkamus priežiūros veiksmus ir kiekvienai rizikos kategorijai rekomenduojamas priemonės, pavyzdžiui, patikrinimų vietoje arba tikslinių saugumo auditų ar saugumo patikrinimų naudojimą, dažnumą ar rūšį, reikalaujamos pateikti informacijos rūšį ir tos informacijos išsamumo lygį. Kartu su tokiais priežiūros metodikomis taip pat gali būti parengiamos darbo programos ir jos gali būti reguliariai vertinamos bei peržiūrimos, be kita ko, atsižvelgiant į tokius aspektus kaip išteklių paskirstymas ir poreikiai;**
- (70aa) viešojo administravimo subjektų atžvilgiu priežiūros įgaliojimais turėtų būti naudojamosi laikantis nacionalinių sistemų ir teisinės tvarkos. Valstybės narės turėtų galėti nuspręsti dėl tinkamų, proporcingų ir veiksmingų priežiūros ir vykdymo užtikrinimo priemonių nustatymo šių subjektų atžvilgiu;**
- (70aaa) valstybės narės galėtų reikalauti, kad esminiai ir svarbūs subjektai, siekdami įrodyti, kad laikosi tam tikrų kibernetinio saugumo rizikos valdymo priemonių, naudotųsi Reglamentu (ES) Nr. 910/2014 nustatytais kvalifikuotomis patikimumo užtikrinimo paslaugomis arba elektroninės atpažinties schemomis, apie kurias pranešta;**

- (71) kad vykdymo užtikrinimas būtų veiksmingas, turėtų būti parengtas būtinas administracinių sankcijų už šioje direktyvoje nustatytą 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;
- (71a) nuostatomis, susijusiomis su fizinių asmenų, vykdančių tam tikras pareigas subjekte, atsakomybe už jų pareigos užtikrinti šioje direktyvoje nustatytų pareigų vykdymą pažeidimą, nereikalaujama, kad valstybės narės užtikrintų baudžiamąjį persekiojimą arba civilinę atsakomybę už dėl tokio pažeidimo padarytą žalą trečiosioms šalims;**
- (72) siekiant užtikrinti veiksmingą šioje direktyvoje nustatytų pareigų vykdymą, kiekvienai kompetentingai institucijai turėtų būti suteikti įgaliojimai skirti administracines baudas arba prašyti jas skirti;

- (73) jei administracinės baudos skiriamos įmonei, tais tikslais įmonė turėtų būti suprantama kaip įmonė, apibrėžta SESV 101 ir 102 straipsniuose. Jei administracinės baudos skiriamos asmenims, kurie nėra įmonė, svarstydama, koks būtų tinkamas baudos dydis, priežiūros institucija turėtų atsižvelgti į bendrą pajamų lygį valstybėje narėje ir į to asmens ekonominę padėtį. Valstybės narės turėtų nustatyti, ar ir koku mastu valdžios institucijoms turėtų būti skiriamos administracinės baudos. Administracinės baudos skyrimas neturi įtakos kompetentingų institucijų kitų įgaliojimų ar kitų sankcijų, nustatytų nacionalinėse taisyklėse, kuriomis ši direktyva perkeliama į nacionalinę teisę, taikymui;
- (74) valstybės narės [...] **gali** nustatyti taisykles dėl baudžiamųjų sankcijų už nacionalinių taisyklių, kuriomis ši direktyva perkeliama į nacionalinę teisę, pažeidimus. Tačiau skiriant baudžiamąsias sankcijas už tokių nacionalinių taisyklių pažeidimus ir susijusias administracines sankcijas neturėtų būti pažeistas *ne bis in idem* principas, kaip jį aiškina Teisingumo Teismas;
- (75) kai šia direktyva administracinės sankcijos nėra suderintos arba kai tai yra būtina kitais atvejais, pavyzdžiui, kai šiurkščiai pažeidžiamos šioje direktyvoje nustatytos pareigos, valstybės narės turėtų įgyvendinti sistemą, pagal kurią numatomos veiksmingos, proporcingos ir atgrasomosios sankcijos. Tokių sankcijų – baudžiamųjų ar administracinių – pobūdis turėtų būti nustatytas valstybės narės teisėje;

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

- (77) šia direktyva turėtų būti nustatytos kompetentingų institucijų ir priežiūros institucijų bendradarbiavimo taisyklės pagal Reglamentą (ES) 2016/679, siekiant kovoti su pažeidimais, susijusiais su asmens duomenimis;
- (78) šia direktyva turėtų būti siekiama užtikrinti aukšto lygio atsakomybę už kibernetinio saugumo rizikos valdymo priemones ir pareigas pranešti organizacijų lygmeniu. Dėl šių priežasčių subjektų, kuriems taikoma ši direktyva, valdymo organai turėtų patvirtinti kibernetinio saugumo rizikos priemones ir prižiūrėti jų įgyvendinimą;
- (79) turėtų būti nustatyta tarpusavio [...] **mokymosi [...] sistema, kuri padėtų stiprinti tarpusavio pasitikėjimą ir mokytis iš gerosios praktikos bei patirties**, sudarant sąlygas valstybių narių paskirtiems ekspertams [...] **tarpusavyje keistis informacija apie [...]** kibernetinio saugumo politikos įgyvendinimą[...]. **Įgyvendinant tarpusavio mokymosi sistemą ypač daug dėmesio turėtų būti skiriama užtikrinimui, kad šia sistema atitinkamoms valstybių narių institucijoms nebūtų užkrauta bereikalinga ar neproporcinga našta. Komisija turėtų išnagrinėti visas galimybes potencialiai užtikrinti finansavimą išlaidoms, kurių gali atsirasti organizuojant tarpusavio mokymosi misijas, padengti. Be to, įgyvendinant tarpusavio mokymosi sistemą turėtų būti atsižvelgiama į panašių mechanizmų, pavyzdžiui, CSIRT tinklo tarpusavio vertinimo sistemos, rezultatus, kuriama pridėtinė vertė ir vengiama dubliavimo. Tarpusavio mokymosi sistemos įgyvendinimas turėtų nedaryti poveikio nacionalinės ar Sąjungos teisės aktams dėl konfidencialios ir įslaptintos informacijos apsaugos. Prieš pradedant tarpusavio mokymosi raundus, valstybės narės gali atlikti su atitinkamais aspektais susijusį įsivertinimą. Bendradarbiavimo grupės prašymu ENISA prireikus gali pateikti gaires dėl įsivertinimo ir atitinkamų šablonų. Valstybės narės galėtų nuspręsti savo atitinkamas ataskaitas skelbti viešai;**

(80) [...]

- (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, **subjektų, iš kurių turi būti reikalaujama naudoti tam tikrus sertifikuotus IRT produktus, paslaugas ir procesus, kategorijomis**, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai. Tais įgaliojimais turėtų būti naudojamosi laikantis Europos Parlamento ir Tarybos reglamento (ES) Nr. 182/2011²⁶;
- (82) Komisija, konsultuodamasi su suinteresuotosiomis šalimis, turėtų periodiškai peržiūrėti šią direktyvą, visų pirma siekdama nustatyti, ar reikia ją keisti atsižvelgiant į kintančias visuomenines, politines, technologines ar rinkos sąlygas;

²⁶ 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).

- (83) kadangi šios direktyvos tikslo, t. y. užtikrinti aukštą bendrą kibernetinio saugumo lygį Sąjungoje, valstybės narės negali deramai pasiekti, o dėl siūlomo veiksmo poveikio to tikslo būtų geriau siekti Sąjungos lygmeniu, laikydamosi Europos Sąjungos sutarties 5 straipsnyje nustatyto subsidarumo principo Sąjunga gali patvirtinti priemones. Pagal tame straipsnyje nustatytą proporcingumo principą šia direktyva neviršijama to, kas būtina nurodytam tikslui pasiekti;
- (84) šia direktyva gerbiamos pagrindinės teisės ir laikomasi principų, pripažintų Europos Sąjungos pagrindinių teisių chartijoje, visų pirma teisė į privatą gyvenimą ir komunikacijos slaptumą, teisė į asmens duomenų apsaugą, laisvė užsiimti verslu, teisė į nuosavybę, teisė į veiksmingą teisinę gynybą ir teisė būti išklausytam. Ši direktyva turėtų būti įgyvendinta atsižvelgiant į tas teises ir principus,

PRIĖMĖ ŠIĄ DIREKTYVĄ:

I SKYRIUS

Bendrosios nuostatos

1 straipsnis

Dalykas

1. Šia direktyva nustatomos priemonės, kuriomis siekiama užtikrinti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje, **kad būtų pagerintas vidaus rinkos veikimas.**
2. Todėl šia direktyva nustatomos:
 - a) valstybių narių pareigos priimti nacionalines kibernetinio saugumo strategijas, paskirti kompetentingas nacionalines institucijas, bendruosius informacinius centrus ir reagavimo į kompiuterių saugumo incidentus tarnybas (CSIRT);
 - b) kibernetinio saugumo rizikos valdymo pareigos ir pareigos pranešti, taikomos [...] **I ir II prieduose** [...] nurodytų rūšių subjektams;
 - c) dalijimosi kibernetinio saugumo informacija **taisyklės ir** pareigos ja dalytis.

2 straipsnis

Taikymo sritis

1. Ši direktyva taikoma [...] **I ir II** prieduose [...] **išvardytų rūšių** viešiesiems ir privatiems subjektams [...], **kurie atitinka arba viršija vidutinėms įmonėms nustatytas viršutines ribas**, kaip tai suprantama Komisijos rekomendacijoje 2003/361/EB²⁷. **Tos rekomendacijos priedo 3 straipsnio 4 dalis ir 6 straipsnio 2 dalies antra ir trečia pastraipos šios direktyvos tikslais netaikomos.**
2. [...] Nepaisant [...] **1 dalyje nurodytų subjektų dydžio**, ši direktyva taip pat taikoma tais atvejais, **kai:** [...]
 - a) paslaugas teikia vienas iš toliau išvardytų subjektų:
 - (i) viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų **teikėjai**, nurodyti I priedo 8 punkte;
 - (ii) **kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai**, nurodyti I priedo **XX punkte**;
 - (iii) **nekvalifikuoti patikimumo užtikrinimo paslaugų teikėjai**, nurodyti I priedo **XX punkte**;
 - iv) aukščiausio lygio domenų vardų registrai [...], nurodyti I priedo 8 punkte;
 - b) [...]

²⁷ 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).

- c) subjektas yra vienintelis paslaugos [...], **kuri yra būtina siekiant užtikrinti ypatingos svarbos visuomeninės ar ekonominės veiklos vykdymą**, teikėjas valstybėje narėje;
- d) potencialus paslaugos, kurią teikia subjektas, sutrikimas galėtų turėti [...] **didelį** poveikį viešajam saugumui, visuomenės saugumui arba visuomenės sveikatai;
- e) potencialus paslaugos, kurią teikia subjektas, sutrikimas galėtų kelti [...] **didele** sistemine riziką visų pirma sektoriuose, kuriuose toks sutrikimas galėtų turėti tarpvalstybinį poveikį;
- f) [...];
- g) nustatoma, kad subjektas yra ypatingos svarbos subjektas pagal Europos Parlamento ir Tarybos direktyvą (ES) XXXX/XXXX²⁸ [Ypatingos svarbos subjektų atsparumo direktyva] [arba kad subjektas yra lygiavertis ypatingos svarbos subjektui pagal tos direktyvos 7 straipsnį].

2a. Ši direktyva taip pat taikoma centrinės valdžios viešojo administravimo subjektams, nepaisant jų dydžio, kurie valstybėje narėje pagal nacionalinę teisę yra pripažįstami tokiais subjektais ir nurodyti I priedo 9 punkte. Valstybės narės gali nustatyti, kad ši direktyva taip pat taikoma viešojo administravimo subjektams regionų ir vietos lygmenimis.

²⁸ [įrašyti visą pavadinimą ir OL paskelbimo nuorodą, kai ji bus žinoma]

3. [...]

Ši direktyva nedaro poveikio valstybių narių atsakomybei užtikrinti nacionalinį saugumą arba jų įgaliojimams apsaugoti kitas esmines valstybines funkcijas, įskaitant valstybės teritorinio vientisumo užtikrinimą ir viešosios tvarkos palaikymą.

3a. 1) Ši direktyva netaikoma:

- a) subjektams, kurie nepatenka į Sąjungos teisės taikymo sritį, ir bet kuriuo atveju visiems subjektams, kurie vykdo veiklą daugiausia gynybos, nacionalinio saugumo, visuomenės saugumo arba teisėsaugos srityse, nepriklausomai nuo to, kuris subjektas vykdo tą veiklą ir ar tai yra viešasis, ar privatusis subjektas, nedarant poveikio 2 punktui;**

- b) subjektams, kurie vykdo veiklą teisminių institucijų, parlamentų arba centrinių bankų veiklos srityse.[...]

2) Kai viešojo administravimo subjektai vykdo veiklą šiose srityse tik kaip savo bendros veiklos dalį, ši direktyva jiems visiškai netaikoma.

3aa. Ši direktyva netaikoma:

- i) subjektų, kurie nepatenka į Sąjungos teisės taikymo sritį, veiklai ir bet kuriuo atveju visai su nacionaliniu saugumu ar gynyba susijusiai veiklai, nepriklausomai nuo to, kuris subjektas vykdo tą veiklą ir ar tai yra viešasis, ar privatusis subjektas;
- ii) subjektų, veikiančių teisminių institucijų, parlamentų, centrinių bankų veiklos srityse ir visuomenės saugumo srityje, veiklai, įskaitant viešojo administravimo subjektus, kurie vykdo teisėsaugos veiklą nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais, veiklai.

3aaa. Šioje direktyvoje nustatytos pareigos nereiškia, kad bus teikiama informacija, kurios atskleidimas prieštarauja esminiams valstybių narių nacionalinio saugumo, visuomenės saugumo ar gynybos interesams.

3aaaa. Ši direktyva nedaro poveikio Sąjungos teisei dėl asmens duomenų apsaugos, visų pirma Reglamentui (ES) 2016/679 ir Direktyvai 2002/58/EB.

3b. Ši direktyva netaikoma subjektams, kuriems netaikomas Europos Parlamento ir Tarybos reglamentas (ES) XXXX/XXXX [DORA reglamentas], vadovaujantis DORA reglamento 2 straipsnio 4 dalimi.

4. Ši direktyva taikoma nedarant poveikio [...] ²⁹ Europos Parlamento ir Tarybos direktyvoms 2011/93/ES ³⁰ ir 2013/40/ES ³¹.

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

²⁹ [...]

³⁰ 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 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).

2a straipsnis

Esminiai ir svarbūs subjektai

1. Iš subjektų, kuriems taikoma ši direktyva, esminiais subjektais laikomi:
 - i) šios direktyvos I priedo 1–8a punktuose ir 10 punkte numatytų rūšių subjektai, kurie viršija vidutinėms įmonėms nustatytas viršutines ribas, kaip apibrėžta Komisijos rekomendacijoje 2003/361/EB;
 - ii) 2 straipsnio 2 dalies a punkto i papunktyje nurodyti vidutinio dydžio subjektai;
 - iii) šios direktyvos 2 straipsnio 2 dalies a punkto ii ir iv papunkčiuose nurodyti subjektai, nepriklausomai nuo jų dydžio;
 - iv) šios direktyvos 2 straipsnio 2 dalies g punkte ir 2 straipsnio 2a dalyje nurodyti subjektai, nepriklausomai nuo jų dydžio;
 - v) jei juos įsteigė valstybės narės, subjektai, kuriuos valstybės narės prieš įsigaliojant šiai direktyvai pagal Direktyvą (ES) 2016/1148 arba nacionalinę teisę įvardijo kaip esminių paslaugų operatorius;
 - vi) II priede numatytų rūšių subjektai, kurie viršija vidutinėms įmonėms nustatytas viršutines ribas, kaip apibrėžta Komisijos rekomendacijoje 2003/361/EB, ir kurių atžvilgiu valstybės narės, remdamosi 2 straipsnio 2 dalies c–e punktuose nurodytais kriterijais, nustato, kad jie yra esminiai subjektai;

- vii) vidutinio dydžio subjektai, kaip tai suprantama Komisijos rekomendacijoje 2003/361/EB, kurių atžvilgiu valstybės narės, remdamosi 2 straipsnio 2 dalies c–e punktuose nurodytais kriterijais, nustato, kad jie yra esminiai subjektai;
- viii) labai maži arba mažieji subjektai, kaip tai suprantama Komisijos rekomendacijoje 2003/361/EB, numatyti šio straipsnio 2 dalies a punkto i papunktyje arba nustatyti pagal šio straipsnio 2 dalies c–e punktus, kurių atžvilgiu valstybės narės, remdamosi nacionaliniais rizikos vertinimais, nustato, kad jie yra esminiai subjektai.

2. Iš subjektų, kuriems taikoma ši direktyva, svarbiais subjektais laikomi:

- i) šios direktyvos I priede numatytų rūšių subjektai, kurie laikomi vidutinėmis įmonėmis, kaip tai suprantama Komisijos rekomendacijoje 2003/361/EB, ir II priede numatytų rūšių subjektai, kurie atitinka arba viršija vidutinėms įmonėms nustatytas viršutines ribas, kaip tai suprantama Komisijos rekomendacijoje 2003/361/EB³²;
- ii) šios direktyvos 2 straipsnio 2 dalies a punkto iii papunktyje nurodyti subjektai, nepriklausomai nuo jų dydžio;
- iii) 2 straipsnio 2 dalies a punkto i papunktyje nurodyti mažieji ir labai maži subjektai;
- iv) mažieji ir labai maži subjektai, kurių atžvilgiu valstybės narės, remdamosi 2 straipsnio 2 dalies c–e punktais, nustato, kad jie yra svarbūs subjektai.

³² 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).

2a straipsnis

Pranešimo mechanizmai

1. Valstybės narės gali nustatyti nacionalinius pranešimo apie save mechanizmus, pagal kuriuos būtų reikalaujama, kad visi subjektai, kuriems taikoma ši direktyva, pagal šią direktyvą kompetentingoms institucijoms arba šiuo tikslu valstybių narių paskirtoms įstaigoms pateiktų bent savo vardą ir pavardę (pavadinimą), adresą ir kontaktinius duomenis, nurodytų sektorių, kuriame jie veikia, arba paslaugų, kurias jie teikia, rūšį, taip pat, kai taikytina, valstybių narių, kuriose jie teikia paslaugas pagal šią direktyvą, sąrašą.
2. Kiek tai susiję su valstybių narių pagal 2 straipsnio 2 dalies b–e punktus nustatytais subjektais, ne vėliau kaip [12 mėnesių po šios direktyvos perkėlimo į nacionalinę teisę termino] valstybės narės [...] pateikia Komisijai bent atitinkamą informaciją apie nustatytų subjektų skaičių, sektorių, kuriame jie veikia, arba paslaugų, kurias jie teikia, rūšį, kaip nurodyta prieduose, taip pat nurodo konkrečią (-ias) 2 straipsnio 2 dalies nuostatą (-as), kuria (-iomis) remiantis jie buvo nustatyti. Valstybės narės reguliariai ir ne rečiau kaip kas dvejus metus peržiūri [...] šią informaciją [...] ir, kai tinkama, ją atnaujina.

2b straipsnis

Konkrečioms sektoriams taikomi Sąjungos aktai

1. Jei pagal [...] konkrečioms sektoriams taikomus **Sąjungos teisės** aktus [...] reikalaujama, kad esminiai arba svarbūs subjektai [...] priimtų kibernetinio saugumo rizikos valdymo priemonės arba praneštų apie **didelius** incidentus ar [...] kibernetines grėsmes, ir jei tų reikalavimai poveikis iš esmės yra bent lygiavertis šioje direktyvoje nustatytų pareigų poveikiui, atitinkamos šios direktyvos nuostatos, **įskaitant VI skyriuje išdėstytas nuostatas dėl priežiūros ir vykdymo užtikrinimo, tokiems subjektams netaikomos. Jei konkrečioms sektoriams taikomi Sąjungos teisės aktai taikomi ne visiems konkrečiam sektoriaus, kuriam taikoma ši direktyva, subjektams, atitinkamos šios direktyvos nuostatos toliau taikomos subjektams, kuriems netaikomos tos konkrečiam sektoriaus nuostatos.**
2. Šio straipsnio 1 dalyje nurodytų reikalavimų poveikis laikomas lygiavertčiu šioje direktyvoje nustatytų pareigų poveikiui, jei atitinkamame konkrečiam sektoriui taikomame Sąjungos akte numatyta, kad pagal šią direktyvą kompetentingos institucijos arba paskirtosios CSIRT gali nedelsiant, o kai tinkama – automatiškai ir tiesiogiai susipažinti su pranešimais apie incidentus, ir jei:
 - a) kibernetinio saugumo rizikos valdymo priemonių poveikis yra bent lygiavertis priemonių, nustatytų šios direktyvos 18 straipsnio 1 ir 2 dalyse, poveikiui arba
 - b) reikalavimų pranešti apie didelius incidentus poveikis yra bent lygiavertis reikalavimų, nustatytų 20 straipsnio 1–6 dalyse, poveikiui.

3. **Komisija periodiškai peržiūri, kaip taikomi šio straipsnio 1 ir 2 dalyse nustatyti reikalavimai dėl lygiaverčio poveikio, kiek tai susiję su konkrečiais sektoriais taikomomis Sąjungos teisės aktų nuostatomis. Rengdama tokias periodines peržiūras Komisija konsultuojasi su Bendradarbiavimo grupe ir ENISA.**

3 straipsnis

Būtinasis suderinimas

Nedarant poveikio kitoms valstybių narių pareigoms pagal Sąjungos teisę, valstybės narės gali [...] srityse, kurioms taikoma ši direktyva, priimti arba išlaikyti nuostatas, kuriomis užtikrinamas aukštesnio lygio kibernetinis saugumas.

4 straipsnis

Apibrėžtys

Šioje direktyvoje vartojamų terminų apibrėžtys:

- 1) tinklų ir informacinė sistema – tai:
 - a) elektroninių ryšių tinklas, kaip tai suprantama Direktyvos (ES) 2018/1972 2 straipsnio 1 punkte;
 - b) bet koks prietaisas arba tarpusavyje sujungtų ar susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė;
 - c) skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami a ir b punktuose nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais;

- 2) tinklų ir informacinių sistemų saugumas – tinklų ir informacinių sistemų pajėgumas tam tikru patikimumo lygiu išlikti atspariems bet kokiam **įvykiui, galinčiam** sukelti pavojų [...] saugomų, perduodamų ar tvarkomų duomenų, arba teikiamų ar per tas tinklų ir informacines sistemas gaunamų paslaugų prieinamumui, autentiškumui, vientisumui arba konfidencialumui;
- 2a) elektroninių ryšių paslaugos – elektroninių[...] ryšių paslaugos, kaip tai suprantama Direktyvos (ES) 2018/1972 2 straipsnio 4 punkte;**
- 3) kibernetinis saugumas – kibernetinis augumas, kaip tai suprantama Europos Parlamento ir Tarybos reglamento (ES) 2019/881³³ 2 straipsnio 1 punkte;
- 4) nacionalinė **kibernetinio saugumo** strategija[...] – nuosekli valstybės narės sistema, kurioje numatomas valdymas siekiant [...]toje valstybėje narėje įgyvendinti strateginius tikslus ir prioritetus [...] **kibernetinio saugumo srityje;**
- 5) incidentas – bet koks įvykis, kuriuo pažeidžiamas saugomų, perduodamų arba tvarkomų duomenų ar [...] paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumas, autentiškumas, vientisumas arba konfidencialumas;
- 5a) didelio masto kibernetinio saugumo incidentas – incidentas, kuris turi reikšmingą poveikį ne mažiau kaip dviem valstybėms narėms arba į kurio sukeltą sutrikimą valstybė narė nepajėgia reaguoti;**

³³ 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 15).

- 6) incidento valdymas – visi veiksmai ir procedūros, kuriais siekiama nustatyti, išanalizuoti ir sustabdyti incidentą, taip pat į jį reaguoti;
- 6a) rizika – potencialus praradimas arba sutrikimas, kurį sukėlė incidentas; ji išreiškiama kaip tokio praradimo arba sutrikimo masto ir to incidento tikimybės derinys;**
- 7) kibernetinė grėsmė – kibernetinė grėsmė, kaip tai suprantama Reglamento (ES) 2019/881 2 straipsnio 8 punkte;
- 7a) didelė kibernetinė grėsmė – kibernetinė grėsmė, kurios atveju, atsižvelgiant į jos technines charakteristikas, galima daryti prielaidą, kad ji gali padaryti didelį neigiamą poveikį subjekto arba jo naudotojų tinklų ir informacinėms sistemoms, sukeldama didelių materialinių arba nematerialinių nuostolių;**
- 8) pažeidžiamumas – IRT turto arba sistemos [...] silpnoji vieta, jautrumas ar trūkumas, kuriais gali būti pasinaudota kibernetinei grėsmei kelti;
- 8a) vos neįvykę incidentai – įvykis, kuris potencialiai galėjo sukelti žalą subjekto arba jo naudotojų tinklų ir informacinėms sistemoms, tačiau faktiniam jo atsitikimui buvo sėkmingai užkirstas kelias;**
- 9) atstovas – bet koks Sąjungoje įsisteigęs fizinis arba juridinis asmuo, paskirtas veikti tik i) DNS paslaugų teikėjo, aukščiausio lygio domenų (TLD) vardų registro, debesijos kompiuterijos paslaugų teikėjo, duomenų centro paslaugų teikėjo, turinio pristatymo tinklo paslaugų teikėjo, kaip apibrėžta I priedo 8 punkte, arba ii) II priedo [...] 6 punkte nurodytų subjektų, kurie nėra įsisteigę Sąjungoje, vardu, į kurį vietoj subjekto dėl to subjekto pareigų pagal šią direktyvą gali kreiptis nacionalinė kompetentinga institucija arba CSIRT;

- 10) standartas – standartas, kaip tai suprantama Europos Parlamento ir Tarybos reglamento (ES) Nr. 1025/2012³⁴ 2 straipsnio 1 punkte;
- 11) techninė specifikacija – techninė specifikacija, kaip tai suprantama Reglamento (ES) Nr. 1025/2012 4 straipsnio 2 punkte;
- 12) interneto duomenų srautų mainų taškas (IXP) – tinklo įrenginys, kuris sudaro sąlygas sujungti daugiau nei du nepriklausomus tinklus (autonomines sistemas), visų pirma siekiant palengvinti interneto duomenų srautų mainus; IXP sujungia tik autonomines sistemas; IXP atveju nėra būtina, kad interneto duomenų srautai, perduodami tarp bet kurių naudojamų autonominių sistemų porų, būtų perduodami per bet kurią trečią autonominę sistemą; be to, jis nekeičia tokių srautų ar kitokiu būdu jų netrikdo;
- 13) domenų vardų sistema (DNS) – hierarchiškai paskirstyta vardų sistema, kuri sudaro sąlygas galutiniams naudotojams gauti paslaugas ir pasinaudoti interneto ištekliais;
- 14) DNS paslaugų teikėjas – subjektas, kuris teikia rekursinio arba patikimo domenų vardų keitimo paslaugas[...] **trečiųjų šalių reikmėms, išskyrus šakninio pavadinimo serverius**[...];

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

- 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, jo duomenų bazių techninę priežiūrą ir aukščiausio lygio domeno zonos rinkmenų paskirstymą tarp vardų serverių, **išskyrus atvejus, kai aukščiausio lygio domenų vardus registras naudoja tik savo reikmėms;**
- 15a) aukščiausio lygio domenų atveju domenų vardų registravimo paslaugas teikiantys subjektai – aukščiausio lygio domeno vardų registrai, aukščiausio lygio domenų registratoriai ir registratorių atstovai, pavyzdžiui, perpardavėjai ir atstovavimo paslaugų teikėjai;**
- 16) skaitmeninė paslauga – paslauga, kaip tai suprantama Europos Parlamento ir Tarybos direktyvos (ES) 2015/1535³⁵ 1 straipsnio 1 dalies b punkte;
- 16a) patikimumo užtikrinimo paslaugos – patikimumo užtikrinimo paslaugos, kaip tai suprantama Reglamento (ES) Nr. 910/2014 3 straipsnio 16 punkte;**

³⁵ 2015 m. rugsėjo 9 d. Europos Parlamento ir Tarybos direktyva (ES) 2015/1535, kuria nustatoma informacijos apie techninius reglamentus ir informacinės visuomenės paslaugų taisyklės teikimo tvarka (OL L 241, 2015 9 17, p. 1).

- 16b) kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas – kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, kaip tai suprantama Reglamento (ES) Nr. 910/2014 3 straipsnio 20 punkte;
- 17) elektroninė prekyvietė – skaitmeninė paslauga, kaip tai suprantama Europos Parlamento ir Tarybos direktyvos 2005/29/EB³⁶ 2 straipsnio n punkte;
- 18) interneto paieškos sistema – skaitmeninė paslauga, kaip tai suprantama Europos Parlamento ir Tarybos reglamento (ES) 2019/1150³⁷ 2 straipsnio 5 punkte;
- 19) debesijos kompiuterijos paslauga – skaitmeninė paslauga, kuri pagal poreikį suteikia administravimo paslaugas ir plataus masto nuotolinę prieigą prie kintamo masto pritaikomos bendrų [...] kompiuterijos išteklių bazės, **įskaitant atvejus, kai šie ištekliai yra paskirstyti per kelias vietas;**
- 20) duomenų centro paslauga – paslauga, kuri apima struktūras arba struktūrų grupes, skirtas informacinių technologijų ir tinklo įrangos centralizuotam pritaikymui, tarpusavio junglumui ir eksploatavimui, teikiant duomenų saugojimo, tvarkymo ir transportavimo paslaugas kartu su visa energijos paskirstymo ir aplinkos kontrolės įranga ir infrastruktūra;

³⁶ 2005 m. gegužės 11 d. Europos Parlamento ir Tarybos direktyva 2005/29/EB dėl nesąžiningos įmonių komercinės veiklos vartotojų atžvilgiu vidaus rinkoje ir iš dalies keičianti Tarybos direktyvą 84/450/EEB, Europos Parlamento ir Tarybos direktyvas 97/7/EB, 98/27/EB bei 2002/65/EB ir Europos Parlamento ir Tarybos reglamentą (EB) Nr. 2006/2004 („Nesąžiningos komercinės veiklos direktyva“) (OL L 149, 2005 6 11, p. 22).

³⁷ 2019 m. birželio 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/1150 dėl verslo klientams teikiamų internetinių tarpininkavimo paslaugų sąžiningumo ir skaidrumo didinimo (OL L 186, 2019 7 11, p. 57).

- 21) turinio teikimo tinklas – geografiškai paskirstytų serverių tinklas, kurio paskirtis yra turinio ir paslaugų teikėjų vardu užtikrinti interneto naudotojams didelę skaitmeninio turinio ir paslaugų pasiūlą, prieinamumą arba greitą teikimą;
- 22) socialinių tinklų paslaugų platforma – platforma, kurioje galutiniams naudotojams sudaromos sąlygos prisijungti, dalytis, rasti vienas kitą ir bendrauti naudojant įvairius prietaisus, visų pirma per pokalbius, įrašus, vaizdo įrašus ir rekomendacijas[...];
- 23) viešojo administravimo subjektas – valstybės narės subjektas, **kuris valstybėje narėje pagal nacionalinę teisę yra pripažįstamas tokiu subjektu [...]** ir kuris atitinka šiuos kriterijus:
- a) yra įsteigtas siekiant tikslo – tenkinti visuotinės svarbos poreikius, kurie nėra pramoninio ar komercinio pobūdžio;
 - b) turi juridinio asmens statusą **arba pagal teisės aktus turi teisę veikti kito juridinio asmens statusą turinčio subjekto vardu;**
 - c) didžiąja dalimi yra finansuojamas valstybės, regionų valdžios institucijos ar kitų viešosios teisės reglamentuojamų įstaigų lėšomis; arba jam taikoma tų institucijų ar įstaigų administracinė priežiūra; arba turi administracinę, valdymo ar priežiūros organą, kurio daugiau kaip pusę narių skiria valstybės, regionų valdžios institucijos arba kitos viešosios teisės reglamentuojamos įstaigos;
 - d) turi įgaliojimus priimti administracinius arba reguliavimo sprendimus dėl fizinių arba juridinių asmenų, kurie daro poveikį jų teisėms atsižvelgiant į tarpvalstybinį asmenų, prekių, paslaugų ar kapitalo judėjimą;
- 24) subjektas – bet kuris fizinis arba juridinis asmuo, įsteigtas ir tokiu pripažintas pagal jo įsteigimo vietos nacionalinę teisę, kuris, veikdamas savo vardu, gali įgyvendinti teises ir kuriam gali būti taikomos pareigos;

- 25) esminis subjektas – **I priede numatytos rūšies subjektas, [...] laikomas „esminiu“ pagal 2a straipsnio 1 dalį;**
- 26) svarbus subjektas – **I ir II prieduose numatytos rūšies subjektas, [...] laikomas „svarbiu“ pagal 2a straipsnio 2 dalį;**
- 26a) IRT produktas – **IRT produktas, kaip tai suprantama Reglamento (ES) 2019/881 2 straipsnio 12 punkte;**
- 26aa) IRT paslauga – **IRT paslauga, kaip tai suprantama Reglamento (ES) 2019/881 2 straipsnio 13 punkte;**
- 26ab) IRT procesas – **IRT procesas, kaip tai suprantama Reglamento (ES) 2019/881 2 straipsnio 14 punkte;**
- 26ac) valdomų paslaugų teikėjas – **subjektas, teikiantis tokias paslaugas kaip tinklo, taikomųjų programų, infrastruktūros ir saugumo paslaugos, užtikrindamas nuolatinį ir reguliary valdymą, paramą ir aktyvų administravimą klientų patalpose, savo MSP duomenų centre (priegloba) arba trečiosios šalies duomenų centre;**
- 26ad) valdomų saugumo paslaugų teikėjas – **subjektas, teikiantis užsakomąsias saugumo priemonių ir sistemų stebėjimo ir valdymo paslaugas. Bendrosios paslaugos apima valdomos užkardos, įsibrovimo aptikimo, virtualiojo privačiojo tinklo, pažeidžiamumų paieškos ir antivirusines paslaugas.**
- Jos taip pat apima naudojimąsi didelio prieinamumo saugumo operacijų centrais (iš savo patalpų arba iš kitų duomenų centrų teikėjų), kad visą parą būtų teikiamos paslaugos, skirtos sumažinti veiklos saugumo personalo, kurį įmonei reikia samdyti, mokyti ir išlaikyti, kad būtų palaikoma priimtina saugumo būklė, skaičių.**

II SKYRIUS

Koordinuotos kibernetinio saugumo reguliavimo sistemos

5 straipsnis

Nacionalinė kibernetinio saugumo strategija

1. Kiekviena valstybė narė priima nacionalinę kibernetinio saugumo strategiją, kurioje apibrėžiami strateginiai tikslai ir tinkamos politikos bei reguliavimo priemonės, kad būtų pasiektas ir išlaikytas aukšto lygmens kibernetinis saugumas. Nacionalinėje kibernetinio saugumo strategijoje visų pirma pateikiama:
 - a) valstybių narių kibernetinio saugumo strategijos tikslai ir prioritetai [...];
 - b) valdymo sistema, kad būtų pasiekti tie tikslai ir įgyvendinti prioritetai, įskaitant 2 dalyje nurodytą politiką ir įvairių institucijų bei subjektų, dalyvaujančių įgyvendinant strategiją [...], vaidmenis ir pareigas;
 - c) [...] **gairės** siekiant nustatyti atitinkamus objektus ir **įvertinti** kibernetinio saugumo riziką toje valstybėje narėje;
 - d) nustatytos parengties, reagavimo į incidentus ir atkūrimo priemonės, įskaitant viešojo ir privačiojo sektorių bendradarbiavimą;
 - e) [...]

f) politikos sistema, padedanti užtikrinti geresnį kompetentingų institucijų pagal šią direktyvą ir Europos Parlamento ir Tarybos direktyvą (ES) XXXX/XXXX³⁸ [Ypatingos svarbos infrastruktūros objektų apsaugos direktyva] veiksmų koordinavimą siekiant **atitinkamai** dalytis informacija apie **kibernetinio saugumo riziką**, [...] kibernetines grėsmes **ir incidentus, taip pat apie nekibernetinę riziką, grėsmes ir incidentus**, ir vykdyti priežiūros užduotis;

fa) politikos sistema, skirta kompetentingų institucijų pagal šią direktyvą ir kompetentingų institucijų, paskirtų pagal konkreitiems sektoriams taikomus teisės aktus, veiksmams koordinuoti ir joms bendradarbiauti.

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

- a) politiką dėl kibernetinio saugumo klausimų IRT produktų ir paslaugų, kuriuos [...] subjektai naudoja teikdami savo paslaugas, tiekimo grandinėje;
- b) **politiką** [...] dėl su kibernetiniu saugumu susijusių reikalavimų, taikomų IRT produktams ir paslaugoms viešuosiuose pirkimuose, **įskaitant kibernetinio saugumo sertifikavimą**, įtraukimo ir tokių reikalavimų specifikacijų;
- c) politiką **dėl pažeidžiamumų valdymo, apimančio** [...] **savanoriško** suderinto pažeidžiamumų atskleidimo, kaip tai suprantama 6 straipsnio **1 dalyje, skatinimą ir sąlygų jam sudarymą**;
- d) politiką, susijusią su bendru atvirojo interneto viešojo pagrindo prieinamumu, [...] vientisumu **ir konfidencialumu**;
- e) politiką dėl **švietimo ir mokymo kibernetinio saugumo srityje** ir kibernetinio saugumo įgūdžių, informuotumo didinimo bei mokslinių tyrimų ir plėtros iniciatyvų skatinimo ir plėtojimo;

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

- f) politiką dėl akademinių ir mokslinių tyrimų institucijų rėmimo siekiant plėtoti kibernetinio saugumo priemones ir saugią tinklų infrastruktūrą;
 - g) politiką, atitinkamas procedūras ir tinkamas dalijimosi informacija priemones siekiant remti savanorišką dalijimąsi kibernetinio saugumo informacija tarp įmonių laikantis Sąjungos teisės;
 - h) politiką, kuria sprendžiami konkretūs MVI, visų pirma į šios direktyvos taikymo sritį nepatenkančių MVI, poreikiai, ir pateikiamos gairės bei parama joms gerinant savo atsparumą kibernetinėms [...] grėsmėms.
3. Valstybės narės per tris mėnesius nuo savo nacionalinių kibernetinio saugumo strategijų priėmimo apie jas informuoja Komisiją. **Tai darydamos** valstybės narės gali nepranešti apie su [...] nacionaliniu saugumu **susijusius strategijos elementus**.
4. Valstybės narės, remdamosi pagrindiniais veiklos rezultatų rodikliais, reguliariai ir ne rečiau kaip kas [...] **penkerius** metus vertina savo nacionalines kibernetinio saugumo strategijas ir prireikus jas keičia. Europos Sąjungos kibernetinio saugumo agentūra (ENISA) valstybėms narėms paprašius padeda **joms** parengti nacionalinę strategiją ir pagrindinius veiklos rezultatų rodiklius, kuriais remiantis įvertinama strategija.

Suderintas pažeidžiamumų atskleidimas ir Europos pažeidžiamumų registras

1. Kiekviena valstybė narė paskiria vieną iš savo CSIRT, kaip nurodyta 9 straipsnyje, koordinuoti suderintą pažeidžiamumų atskleidimą. Paskirtoji CSIRT veikia kaip patikimas tarpininkas, prireikus lengvinantis sąveiką tarp pranešimą teikiančio subjekto, **potencialaus pažeidžiamumo savininko** ir IRT produktų gamintojo ar IRT paslaugų teikėjo. **Kiekvienas fizinis ar juridinis asmuo paskirtajai CSIRT gali pranešti (galbūt anonimiškai) apie 4 straipsnio 8 dalyje nurodytą pažeidžiamumą. Paskirtoji CSIRT užtikrina deramus tolesnius veiksmus, susijusius su pranešimu, ir asmens, kuris praneša apie pažeidžiamumą, tapatybės konfidencialumą.** Jeigu pažeidžiamumas, apie kurį pranešta, [...] galėtų potencialiai daryti didelį poveikį subjektams daugiau nei vienoje valstybėje narėje, kiekvienos valstybės narės atitinkama paskirtoji CSIRT, **kai tinkama**, CSIRT tinkle bendradarbiauja su **kitomis paskirtosiomis CSIRT**.
2. ENISA, **konsultuodamasi su Bendradarbiavimo grupe**, 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 **savanoriškai** atskleisti ir registruoti **viešai žinomus** IRT produktų ar IRT 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 IRT 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 **nacionalinių kompetentingų institucijų arba CSIRT parengtas** gaires, kaip galima sumažinti atskleistų pažeidžiamumų keliamą riziką. **ENISA užtikrina, kad Europos pažeidžiamumų registrui būtų naudojama saugi ir atspari ryšių ir informacinė infrastruktūra.**

Nacionalinės kibernetinio saugumo krizės valdymo sistemos

1. Kiekviena valstybė narė paskiria vieną arba daugiau kompetentingų institucijų, kurios atsako už didelio masto **kibernetinio saugumo** incidentų ir krizių valdymą. Valstybės narės užtikrina, kad kompetentingos institucijos turėtų pakankamai išteklių, reikalingų veiksmingam ir efektyviam joms pavestų užduočių vykdymui. **Valstybės narės užtikrina suderinamumą su esamomis bendro krizių valdymo sistemomis.**
2. Kiekviena valstybė narė, taikydama šią direktyvą, nustato pajėgumus, objektus ir procedūras, kuriais galima pasinaudoti krizės atveju.
3. Kiekviena valstybė narė priima nacionalinį reagavimo į kibernetinio saugumo incidentus ir krizę planą, kuriame išdėstomi didelio masto kibernetinio saugumo incidentų ir krizių valdymo tikslai ir būdai. Plane visų pirma nustatomi:
 - a) nacionalinių pasirengimo priemonių ir veiksmų tikslai;
 - b) nacionalinių kompetentingų institucijų užduotys ir pareigos;
 - c) kibernetinio saugumo krizių valdymo procedūros, **įskaitant jų integravimą į nacionalinę bendro krizių valdymo sistemą** ir keitimosi informacija kanalai;
 - d) pasirengimo priemonės, įskaitant reguliarias pratybas ir mokymo veiklą;
 - e) atitinkamos viešosios ir privačiosios [...] šalys ir naudojama infrastruktūra;
 - f) atitinkamų nacionalinių institucijų ir įstaigų nacionalinės procedūros ir susitarimai, kuriais siekiama užtikrinti, kad valstybė narė veiksmingai dalyvautų vykdant koordinuotą didelio masto kibernetinio saugumo incidentų ir krizių valdymą Sąjungos lygmeniu ir jį remtų.

4. Valstybės narės [...] **informuoja** Komisiją **apie** jų kompetentingų institucijų paskyrimą, kaip nurodyta 1 dalyje, ir pateikia **aktualią informaciją, susijusią su šio straipsnio 3 dalies reikalavimais, taikomais** jų nacionaliniams reagavimo į kibernetinio saugumo incidentus ir krizes planams, [...] per tris mėnesius nuo tokio paskyrimo ir tų planų priėmimo. Valstybės narės [...] gali tam tikros informacijos nenurodyti, jeigu tai yra [...] būtina jų nacionaliniam saugumui, **visuomenės saugumui ar gynybai**.

8 straipsnis

Nacionalinės kompetingos institucijos ir bendrieji informaciniai centrai

1. Kiekviena valstybė narė paskiria vieną arba daugiau kompetentingų institucijų, atsakingų už kibernetinį saugumą ir šios direktyvos VI skyriuje nustatytų priežiūros užduočių vykdymą. Valstybės narės šiuo tikslu gali paskirti jau veikiančią instituciją arba institucijas.
2. 1 dalyje nurodytos kompetingos institucijos stebi šios direktyvos taikymą nacionaliniu lygmeniu.
3. Kiekviena valstybė narė paskiria vieną nacionalinį bendrąjį kibernetinio saugumo informacinį centrą (toliau – bendrasis informacinis centras). Kai valstybė narė paskiria tik vieną kompetentingą instituciją, ta kompetentinga institucija taip pat vykdo tos valstybės narės bendrojo informacinio centro funkcijas.
4. Kiekvienas bendrasis informacinis centras vykdo ryšių palaikymo funkciją, kad būtų užtikrintas jo valstybės narės institucijų tarpvalstybinis bendradarbiavimas su atitinkamomis kitų valstybių narių institucijomis ir tarpsektorinis bendradarbiavimas su kitomis nacionalinėmis kompetentingomis institucijomis valstybėje narėje.

5. Valstybės narės užtikrina, kad 1 dalyje nurodytos kompetentingos institucijos ir bendri informaciniai centrai turėtų tinkamų išteklių, kad veiksmingai ir efektyviai vykdytų jiems pavestas užduotis ir taip įgyvendintų šios direktyvos tikslus. Valstybės narės užtikrina veiksmingą, efektyvų ir saugų į 12 straipsnyje nurodytą Bendradarbiavimo grupę paskirtų atstovų bendradarbiavimą.
6. Kiekviena valstybė narė nepagrįstai nedelsdama praneša Komisijai apie 1 dalyje nurodytą paskirtą kompetentingą instituciją ir 3 dalyje nurodytą bendrąjį informacinį centrą, jų užduotis ir bet kokius vėlesnius jų pakeitimus. Kiekviena valstybė narė apie paskyrimą skelbia viešai. Komisija paskelbia paskirtų bendrųjų informacinių centrų sąrašą.

9 straipsnis

Reagavimo į kompiuterių saugumo incidentus tarnybos (CSIRT)

1. Kiekviena valstybė narė paskiria vieną arba daugiau CSIRT, kurios laikosi 10 straipsnio 1 dalyje išdėstytų reikalavimų, taikomų bent jau I ir II prieduose nurodytiems sektoriams, pasektoriams arba subjektams, ir kurios atsako už incidentų valdymą pagal aiškiai apibrėžtą procesą. CSIRT gali būti įsteigta kompetentingoje institucijoje, kuri nurodyta 8 straipsnyje.
2. Valstybės narės užtikrina, kad kiekviena CSIRT turėtų tinkamų išteklių, kad galėtų veiksmingai vykdyti savo užduotis, nurodytas 10 straipsnio 2 dalyje. **Vykdydamos šias užduotis CSIRT gali suteikti pirmenybę tam tikrų paslaugų subjektams teikimui remiantis rizika grindžiamu požiūriu.**
3. Valstybės narės užtikrina, kad kiekviena CSIRT turėtų tinkamą, saugią ir atsparią ryšių ir informacinę struktūrą, kad galėtų keisti informacija su esminiais ir svarbiais subjektais ir kitomis atitinkamomis suinteresuotosiomis šalimis. Šiuo tikslu valstybės narės užtikrina, kad CSIRT prisidėtų prie saugaus dalijimosi informacija priemonių diegimo.

4. CSIRT pagal 26 straipsnį bendradarbiauja ir, kai tinkama, keičiasi atitinkama informacija su patikimomis sektoriaus arba kelių sektorių esminių ir svarbių subjektų bendruomenėmis.
5. CSIRT dalyvauja tarpusavio [...] **mokymosi veikloje**, kuri rengiama pagal 16 straipsnį.
6. Valstybės narės užtikrina efektyvų, veiksmingą ir saugų jų CSIRT bendradarbiavimą 13 straipsnyje nurodytame CSIRT tinkle.
7. Valstybės narės nepagrįstai nedelsdamos praneša Komisijai apie pagal 1 dalį paskirtas CSIRT, CSIRT koordinatorių, paskirtą pagal 6 straipsnio 1 dalį, ir jų atitinkamas užduotis, kurias jos vykdo I ir II prieduose išvardytų subjektų atžvilgiu.
8. Valstybės narės gali paprašyti ENISA padėti kurti nacionalines CSIRT.

10 straipsnis

CSIRT keliami reikalavimai ir užduotys

1. CSIRT turi atitikti šiuos reikalavimus:
 - a) CSIRT užtikrina, kad jų ryšio [...] **kanalai** būtų lengvai prieinami išvengiant kritinių funkcionavimo trikties taškų, taip pat nustato keletą būdų, kaip bet kuriuo metu susisiekti su jomis ir kitais subjektais. CSIRT aiškiai nurodo ryšių kanalus ir apie juos informuoja savo klientus ir bendradarbiavimo partnerius;
 - b) CSIRT biurai ir pagalbinės informacinės sistemos veikia saugiose vietose;

- c) CSIRT aprūpinamos tinkama prašymų valdymo ir nukreipimo sistema, visų pirma siekiant palengvinti veiksmingą ir efektyvų perdavimą;
- d) CSIRT turi pakankamai darbuotojų, kad būtų užtikrintas pasiekiamumas bet kuriuo metu;
- e) CSIRT aprūpinamos antrinėmis sistemomis ir atsargine darbo erdve, kad būtų užtikrintas jų paslaugų tęstinumas;
- f) CSIRT turi galimybę dalyvauti tarptautiniuose bendradarbiavimo tinkluose.

2. CSIRT vykdo šias užduotis:

- a) stebi kibernetines grėsmes, pažeidžiamumus ir incidentus nacionaliniu lygmeniu;
- b) teikia išankstinius įspėjimus, perspėjimus, pranešimus ir platina informaciją apie kibernetines grėsmes, pažeidžiamumus ir incidentus esminiams ir svarbiems subjektams, taip pat **kompetentingoms institucijoms ir** kitoms atitinkamoms suinteresuotosioms šalims;
- c) reaguoja į incidentus;
- d) renka ir analizuoja teismo ekspertizės duomenis ir teikia dinaminę rizikos ir incidentų analizę, taip pat užtikrina informuotumą apie padėtį kibernetinio saugumo srityje;
- e) [...] proaktyviai tikrina tinklų ir informacines sistemas [...], **kad aptiktų pažeidžiamumus, galinčius daryti didelį poveikį, su sąlyga, kad neturint to subjekto pritarimo į tinklus ir informacines sistemas nesibraunama ir jų veikimui neigiamas poveikis nedaromas;**

- f) dalyvauja CSIRT tinkle ir teikia savitarpio pagalbą **pagal savo pajėgumus ir kompetenciją** kitiems tinklo nariams jų prašymu;
 - fa) **kai taikytina, veikia kaip koordinatorius suderinto pažeidžiamumų atskleidimo proceso pagal 6 straipsnio 1 dalį tikslais; tai apima visų pirma pranešančiųjų subjektų, potencialaus pažeidžiamumo savininko ir IRT produktų gamintojo ar IRT paslaugų teikėjo bendravimo palengvinimą tais atvejais, kai tai būtina, atitinkamų subjektų identifikavimą ir susisiekimą su jais, paramą pranešantiems subjektams, derybas dėl informacijos atskleidimo terminų ir pažeidžiamumų, kurie daro poveikį kelioms organizacijoms, valdymą (daugiašalis suderintas pažeidžiamumų atskleidimas).**
3. CSIRT užmezga bendradarbiavimo ryšius su atitinkamais privačiojo sektoriaus subjektais, kad būtų geriau pasiekti direktyvos tikslai.
- 3a. **CSIRT gali užmegzti bendradarbiavimo ryšius su trečiųjų valstybių nacionalinėmis CSIRT. Vykdydamos šį bendradarbiavimą, jos gali keistis atitinkama informacija, įskaitant asmens duomenis, laikydamosi Sąjungos duomenų apsaugos teisės.**
4. Siekdamos palengvinti bendradarbiavimą, CSIRT skatina priimti ir naudoti bendrą arba standartizuotą praktiką, klasifikavimo sistemas ir taksonomiją srityse, susijusiose su:
- a) incidentų valdymo procedūromis;
 - b) kibernetinio saugumo krizės valdymu;
 - c) suderintu pažeidžiamumų atskleidimu.

Paskelbimas nacionaliniu lygmeniu

1. Kai tos pačios valstybės narės kompetentingos institucijos, nurodytos 8 straipsnyje, bendrasis informacinis centras ir CSIRT yra atskiri, jie bendradarbiauja tarpusavyje, kad vykdytų šioje direktyvoje nustatytas pareigas.
2. Valstybės narės užtikrina, kad jų kompetentingos institucijos arba CSIRT gautų šioje direktyvoje nustatyta tvarka pateikiamus pranešimus apie incidentus, dideles kibernetines grėsmes ir vos neįvykusius incidentus. Jeigu valstybė narė nusprendžia, kad jos CSIRT neturi gauti pranešimų, CSIRT, kiek tai būtina jų užduotims vykdyti, suteikiama prieiga prie duomenų apie incidentus, apie kuriuos pranešė esminiai ar svarbūs subjektai pagal 20 straipsnį.
3. Kiekviena valstybė narė užtikrina, kad jos kompetentingos institucijos arba CSIRT informuotų savo bendrąjį informacinį centrą apie šioje direktyvoje nustatyta tvarka pateikiamus pranešimus apie incidentus, dideles kibernetines grėsmes ir vos neįvykusius incidentus.

4. Tiek, kiek būtina tam, kad šioje direktyvoje nustatytos užduotys ir pareigos būtų vykdomos veiksmingai, valstybės narės užtikrina tinkamą kompetentingų institucijų, **CSIRT**, bendrųjų informacinių centrų, teisėsaugos institucijų, duomenų apsaugos institucijų ir **kompetentingų institucijų, paskirtų [...]** pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva[...]], **kompetentingų institucijų pagal Komisijos įgyvendinimo reglamentą 2019/1583, nacionalinių reguliavimo institucijų, paskirtų pagal Direktyvą (ES) 2018/1972, nacionalinių institucijų, paskirtų pagal Reglamento (ES) Nr. 910/2014 17 straipsnį, [...]**nacionalinių finansų institucijų, paskirtų pagal Europos Parlamento ir Tarybos reglamentą (ES) XXXX/XXXX [DORA reglamentas], **taip pat kompetentingų institucijų, paskirtų pagal kitus konkrečioms sektoriams taikomus Sąjungos teisės aktus, bendradarbiavimą toje valstybėje narėje.**
5. Valstybės narės užtikrina, kad jų kompetentingos institucijos **pagal šią direktyvą ir kompetentingos institucijos, paskirtos pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyvą]**, reguliariai **keistųsi [...]** informacija [...] apie **ypatingos svarbos subjektų identifikavimą, kibernetinio saugumo riziką, kibernetinės grėsmės ir incidentus bei nekibernetinę riziką, grėsmės ir incidentus**, darančius poveikį esminiams subjektams, kurie pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyvą] laikomi ypatingos svarbos subjektais [arba ypatingos svarbos subjektams lygiaverčiais subjektais], taip pat apie priemones, kurių [...] imtasi reaguojant į tą riziką ir incidentus. **Valstybės narės taip pat užtikrina, kad kompetentingos institucijos pagal šią direktyvą [...] ir kompetentingos institucijos, paskirtos pagal Reglamentą XXXX/XXXX [DORA reglamentas], Direktyvą 2018/1972 ir Reglamentą (ES) 910/2014, reguliariai keistųsi atitinkama informacija.**

Patikimumo užtikrinimo paslaugų teikėjų atžvilgiu ir [...] visų pirma, [...] kai tas priežiūros vaidmuo pagal šią direktyvą patikimas kitai įstaigai, o ne priežiūros įstaigoms, paskirtoms pagal Reglamentą (ES) 910/2014, nacionalinės kompetentingos institucijos pagal šią direktyvą glaudžiai ir laiku bendradarbiauja keisdamosi atitinkama informacija, kad būtų užtikrinta veiksminga patikimumo užtikrinimo paslaugų teikėjų priežiūra ir užtikrinimas, kad jie laikytųsi šioje direktyvoje bei Reglamente [XXXX/XXXX] nustatytų reikalavimų, **ir, kai taikytina, nacionalinė kompetentinga institucija pagal šią direktyvą, nepagrįstai nedelsdama, informuoja eIDAS priežiūros įstaigą apie visas dideles kibernetines grėsmes arba incidentus, darančius poveikį patikimumo užtikrinimo paslaugoms, apie kuriuos pranešta.**

- 5a. [...] Siekiant supaprastinti pranešimų apie incidentus teikimą, valstybės narės gali sukurti vieną bendrą prieigą visiems pranešimams, kuriuos reikalaujama pateikti pagal šią direktyvą ir, kai tinkama, pagal Reglamentą (ES) 2016/679 ir Direktyvą 2002/58/EB. Valstybės narės gali naudotis viena bendra prieiga pranešimams, kuriuos reikalaujama pateikti pagal kitus konkrečiams sektoriams taikomus Sąjungos teisės aktus. Šia viena bendra prieiga nedaromas poveikis Reglamento (ES) 2016/679 ir Direktyvos 2002/58/EB nuostatų, visų pirma susijusių su nepriklausomomis priežiūros institucijomis, taikymui.

III SKYRIUS

Bendradarbiavimas ES lygmeniu

12 straipsnis

Bendradarbiavimo grupė

1. Siekiant remti ir palengvinti strateginį bendradarbiavimą ir keitimąsi informacija tarp valstybių narių, **taip pat** [...] **sustiprinti pasitikėjimą ir patikimumą** [...], sudaroma Bendradarbiavimo grupė.
2. Bendradarbiavimo grupė vykdo savo užduotis remdamasi dviemėmis darbo programomis, nurodytomis 6 dalyje.
3. Bendradarbiavimo grupę sudaro valstybių narių, Komisijos ir ENISA atstovai. Europos išorės veiksmų tarnyba Bendradarbiavimo grupėje dalyvauja stebėtojos teisėmis. Europos priežiūros institucijos (EPI) **ir kompetentingos institucijos, paskirtos pagal Reglamentą (ES) XXXX/XXXX [DORA reglamentas]**, [...] gali dalyvauti Bendradarbiavimo grupės veikloje **laikantis Reglamento (ES) XXXX/XXXX [DORA reglamentas] 42 straipsnio 1 dalies**.

Kai tikslinga, Bendradarbiavimo grupė gali pakviesti atitinkamų suinteresuotųjų subjektų atstovus dalyvauti jos darbe.

Komisija teikia sekretoriato paslaugas.

4. Bendradarbiavimo grupė vykdo šias užduotis:
 - a) teikia kompetentingoms institucijoms gaires dėl šios direktyvos perkėlimo į nacionalinę teisę ir įgyvendinimo;
 - aa) **teikia gaires, susijusias su suderinto pažeidžiamumų atskleidimo politikos plėtojimu ir įgyvendinimu, kaip nurodyta 5 straipsnio 2 dalies c punkte ir 6 straipsnio 1 dalyje;**

- b) keičiasi geriausios praktikos pavyzdžiais ir informacija, susijusia su šios direktyvos įgyvendinimu, įskaitant informaciją, susijusią su kibernetinėmis grėsmėmis, incidentais, pažeidžiamumais, vos neįvykusiais incidentais, informuotumo didinimo iniciatyvomis, mokymu, pratybomis ir įgūdžiais, gebėjimų stiprinimu, taip pat standartais ir techninėmis specifikacijomis;
- c) keičiasi patarimais ir bendradarbiauja su Komisija dėl naujų kibernetinio saugumo politikos iniciatyvų;
- d) keičiasi patarimais ir bendradarbiauja su Komisija dėl Komisijos įgyvendinimo [...] aktų, priimtų pagal šią direktyvą, projektų;
- e) keičiasi geriausia patirtimi ir informacija su atitinkamomis Sąjungos institucijomis, įstaigomis, biurais ir agentūromis;
- ea) keičiasi nuomonėmis apie konkrečių sektorių teisės aktų, apimančių kibernetinio saugumo aspektus, įgyvendinimą;**
- f) aptaria 16 straipsnio 7 dalyje nurodytas tarpusavio [...] **mokymosi** ataskaitas;
- g) aptaria bendros priežiūros veiklos tarpvalstybiniais atvejais, kaip nurodyta 34 straipsnyje, [...] **patirtį**;
- h) teikia strategines gaires CSIRT tinklui ir **EU–CyCLONe** konkrečiais kylančiais klausimais;

ha) keičiasi nuomonėmis dėl tolesnių politikos veiksmų, susijusių su didelio masto kibernetinio saugumo incidentais, remiantis CSIRT tinklo ir EU–CyCLONe patirtimi;

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

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

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

ka) pagal šios direktyvos 16 straipsnį nustato tarpusavio mokymosi mechanizmą.

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

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

7. Komisija gali priimti įgyvendinimo aktus, kuriais nustatoma procedūrinė tvarka, būtina Bendradarbiavimo grupės veikimui užtikrinti. Tie įgyvendinimo aktai priimami laikantis 37 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.
8. Bendradarbiavimo grupė reguliariai 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 strateginę bendradarbiavimą ir **palengvintų** keitimąsi informacija.

13 straipsnis

CSIRT tinklas

1. Siekiant prisidėti prie pasitikėjimo ir atsakomybės didinimo, taip pat skatinti greitą ir veiksmingą valstybių narių operatyvinį bendradarbiavimą, sukuriamas CSIRT tinklas.
2. CSIRT tinklą sudaro valstybių narių CSIRT, **paskirtų pagal 9 straipsnį**, ir CERT-EU atstovai. Komisija dalyvauja CSIRT tinklo veikloje stebėtojos teisėmis. ENISA teikia sekretoriato paslaugas ir aktyviai remia CSIRT tarpusavio bendradarbiavimą.
3. CSIRT tinklas vykdo šias užduotis:
 - a) keičiasi informacija apie CSIRT pajėgumus;
 - b) keičiasi atitinkama informacija apie incidentus, vos neįvykusius incidentus, kibernetines grėsmes, riziką ir pažeidžiamumus;

- ba) keičiasi informacija apie kibernetinio saugumo leidinius ir rekomendacijas;
- bb) dalijasi techniniais sprendimais, kurie padeda lengviau techniškai valdyti incidentus;
- bc) keičiasi geriausios praktikos pavyzdžiais, priemonėmis ir procesais, susijusiais su CSIRT užduotimis;
- c) CSIRT tinklo **nario**, kuris galėjo būti paveiktas incidento, [...] prašymu keičiasi informacija, susijusia su tuo incidentu ir atitinkamomis kibernetinėmis grėsmėmis, rizika ir pažeidžiamumais, ir ją aptaria;
- d) CSIRT tinklo [...] **nario** prašymu aptaria ir, kai įmanoma, įgyvendina koordinuotą atsaką į incidentą, nustatytą tos valstybės narės jurisdikcijoje;
- e) teikia valstybėms narėms paramą šalinant tarpvalstybinius incidentus pagal šią direktyvą;
- f) bendradarbiauja, **keičiasi geriausios praktikos pavyzdžiais** ir teikia paramą pagal 6 straipsnį paskirtosioms CSIRT, susijusiai su [...] suderintu pažeidžiamumų, darančių poveikį įvairiems IRT produktų, IRT paslaugų ir IRT procesų gamintojams ar teikėjams, kurie yra įsisteigę įvairiose valstybėse narėse, atskleidimo valdymu;
- g) aptaria ir nustato tolesnes operatyvinio bendradarbiavimo formas, be kita ko, susijusias su:
 - i) kibernetinių grėsmių ir incidentų kategorijomis;
 - ii) išankstiniais įspėjimais;
 - iii) savitarpio pagalba;

- iv) koordinavimo principais ir tvarka reaguojant į tarpvalstybinę riziką ir incidentus;
- v) pagalba rengiant nacionalinį reagavimo į kibernetinio saugumo incidentus ir krizes planą, nurodytą 7 straipsnio 3 dalyje, **teikiama valstybės narės prašymu**;
- h) informuoja Bendradarbiavimo grupę apie savo veiklą ir tolesnes operatyvinio bendradarbiavimo formas, aptartas pagal g punktą, **ir** prireikus prašo šiuo atžvilgiu pateikti rekomendacijų;
- i) naudojami kibernetinio saugumo pratybomis, įskaitant ENISA organizuojamas pratybas;
- j) atskiros CSIRT prašymu aptaria tos CSIRT pajėgumus ir parengtį;
- k) bendradarbiauja ir keičiasi informacija su regioniniais ir Sąjungos lygmens saugumo operacijų centrais (SOC), kad pagerintų bendrą informuotumą apie padėtį, susijusią su incidentais ir grėsmėmis visoje Sąjungoje;
- l) aptaria 16 straipsnio 7 dalyje nurodytas tarpusavio [...] **mokymosi** ataskaitas;
- m) teikia gaires siekiant palengvinti operatyvinės praktikos konvergenciją taikant šio straipsnio nuostatas dėl operatyvinio bendradarbiavimo.

4. 35 straipsnyje nurodytos peržiūros tikslais, ne vėliau kaip praėjus [24 mėnesiams po šios direktyvos įsigaliojimo dienos] ir paskui kas dvejus metus CSIRT tinklas įvertina padarytą pažangą operatyvinio bendradarbiavimo srityje ir parengia ataskaitą. Ataskaitoje visų pirma pateikiamos išvados dėl 16 straipsnyje nurodyto tarpusavio **mokymosi** [...], surengto dėl šiame straipsnyje nurodytų nacionalinių CSIRT, rezultatų, įskaitant išvadas ir rekomendacijas. Ta ataskaita taip pat pateikiama Bendradarbiavimo grupei.
5. CSIRT tinklas priima savo darbo tvarkos taisykles.
6. **CSIRT tinklas su EU-CyCLONe bendradarbiauja remdamasis sutartomis procedūrinėmis taisyklėmis.**

14 straipsnis

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

1. Siekiant remti koordinuotą didelio masto kibernetinio saugumo incidentų ir krizių valdymą veiklos lygmeniu ir užtikrinti reguliarią keitimąsi informacija tarp valstybių narių ir Sąjungos institucijų, įstaigų ir agentūrų, įsteigiamas Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas (EU-CyCLONe).
2. EU-CyCLONe sudaro valstybių narių **kibernetinių** krizių valdymo institucijų, paskirtų pagal 7 straipsnį, [...] atstovai. **Komisija dalyvauja tinklo veikloje stebėtojos teisėmis.** ENISA teikia tinklo sekretoriato paslaugas ir padeda saugiai keistis informacija, **taip pat teikia būtinas saugų keitimąsi informacija užtikrinančias priemones valstybių narių tarpusavio bendradarbiavimui remti.**

Kai tikslinga, EU-CyCLONe gali pakviesti atitinkamų suinteresuotųjų subjektų atstovus dalyvauti savo darbe.

3. EU-CyCLONe vykdo šias užduotis:
- a) didina pasirengimo valdyti didelio masto **kibernetinio saugumo** incidentus ir krizes lygi;
 - b) plėtoja bendrą informuotumą apie padėtį, [...] susijusią su didelio masto kibernetinio saugumo incidentais ir krizėmis;
 - ba) įvertina atitinkamų didelio masto kibernetinio saugumo incidentų pasekmes ir poveikį ir siūlo galimas švelninimo priemones;**
 - c) koordinuoja didelio masto kibernetinio saugumo incidentų ir krizių **valdymą** ir padeda politiniu lygmeniu priimti sprendimus, susijusius su tokiais incidentais ir krizėmis;
 - d) **valstybės narės prašymu** aptaria 7 straipsnio **3** [...] dalyje nurodytus **j**os nacionalinius reagavimo į kibernetinio saugumo incidentus ir **krizes** planus.[...]
4. EU-CyCLONe priima savo darbo tvarkos taisykles.
5. EU-CyCLONe reguliariai informuoja Bendradarbiavimo grupę apie **didelio masto kibernetinio saugumo incidentų ir krizių valdymą** [...], ypač daug dėmesio skirdamas jų poveikiui esminiams ir svarbiems subjektams.
6. EU-CyCLONe su CSIRT tinklu bendradarbiauja remdamasis sutartomis procedūrinėmis taisyklėmis.
7. **Ne vėliau kaip [24 mėnesiai po šios direktyvos įsigaliojimo dienos] EU-CyCLONe pateikia Europos Parlamentui ir Tarybai ataskaitą, kurioje įvertina savo darbą.**

14a straipsnis

Tarptautinis bendradarbiavimas

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

15 straipsnis

Kibernetinio saugumo Sąjungoje būklės ataskaita

1. ENISA, bendradarbiaudama su Komisija **ir Bendradarbiavimo grupe**, kas dvejus metus rengia kibernetinio saugumo Sąjungoje būklės ataskaitą. **Visų pirma** [...] į tą ataskaitą [...] įtraukiama [...]:
 - aa) **Sąjungos lygmens kibernetinio saugumo rizikos vertinimas, kuriame atsižvelgiama į grėsmių padėtį;**
 - a) [...] kibernetinio saugumo pajėgumų plėtojimo viešajame ir privačiajame sektoriuose visoje Sąjungoje **vertinimas;**
 - b) [...]
 - c) **apibendrintas vertinimas, grindžiamas kibernetinio saugumo [...] kiekybiniais ir kokybiniais rodikliais, kuriame pateikiama kibernetinio saugumo pajėgumų, įskaitant konkrečių sektorių pajėgumus, brandos lygio[...] apžvalga.**

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

16 straipsnis

Tarpusavio mokymasis

1. **Siekdama stiprinti tarpusavio pasitikėjimą, pasiekti aukštą bendrą kibernetinio saugumo lygį, taip pat stiprinti valstybių narių kibernetinio saugumo pajėgumus ir politiką, būtinus šiai direktyvai veiksmingai įgyvendinti, [...] Bendradarbiavimo grupė, remiama Komisijos ir pasikonsultavusi su ENISA bei, kai aktualu, CSIRT tinklu, ne vėliau kaip per 24 [...] mėnesius nuo šios direktyvos įsigaliojimo [...] nustato objektyviai, nediskriminacinei ir sąžiningai tarpusavio mokymosi sistemai, susijusiai su valstybių narių vykdomu [...] šios direktyvos įgyvendinimu, [...] skirtą metodiką[...]. Dalyvavimas tarpusavio mokymosi veikloje yra savanoriškas. Sistema yra sudaryta iš vertinimų raundų, [...] kuriuos atlieka kibernetinio saugumo [...] ekspertai, atrinkti iš valstybių narių, [...] ir apima [...] vieną ar kelis iš toliau nurodytų aspektų:**
- i) kibernetinio saugumo rizikos valdymo reikalavimų ir pareigų pranešti, nurodytų 18 ir 20 straipsniuose, įgyvendinimą [...];
 - ii) pajėgumus[...], įskaitant turimus [...] išteklius, ir [...] 8 straipsnyje nurodytų nacionalinių kompetentingų institucijų ir 9 straipsnyje nurodytų CSIRT užduočių vykdymą;

[...]

iii[...]) 34 straipsnyje nurodytos savitarpio pagalbos **įgyvendinimą** [...];

iv) [...] 26 straipsnyje nurodytos keitimosi informacija sistemos **įgyvendinimą**[...].

2. **Kriterijai, kuriais remdamosi valstybės narės paskiria ekspertus, atitinkančius reikalavimus dalyvauti tarpusavio mokymosi raunduose, turi būti**[...] objektyvūs, nediskriminaciniai, sąžiningi bei skaidrūs [...] **ir įtraukti į 1 dalyje nurodytą metodiką.** ENISA ir Komisija [...] **gali** paskirti ekspertus dalyvauti **tarpusavio mokymosi raunduose** [...] stebėtojų teisėmis. [...]
3. [...] .

- 3a. Prieš pradedant tarpusavio mokymosi raundus, valstybės narės gali įsivertinti aspektus, kuriuos apima tas konkretus tarpusavio mokymosi raundas, ir tą įsivertinimą pateikti 2 dalyje nurodytiems paskirtiems ekspertams.
4. Tarpusavio **mokymosi veikla** [...] gali apimti **fizinius** arba virtualius apsilankymus vietoje ir keitimąsi informacija ne vietoje. Atsižvelgiant į gero bendradarbiavimo principą, valstybės narės, [...] **dalyvaujančios tarpusavio mokymosi veikloje**, pateikia paskirtiems ekspertams [...] vertinimui reikalingą informaciją[...]; **tai daroma nedarant poveikio nacionalinės ar Sąjungos teisės aktams dėl konfidencialios ar įslaptintos informacijos apsaugos arba esminių valstybės funkcijų, pavyzdžiui, nacionalinio saugumo, apsaugai**. Visa per tarpusavio **mokymosi** procesą gauta informacija naudojama tik tuo tikslu. Tarpusavio [...] **mokymosi** veikloje dalyvaujantys ekspertai neatskleidžia jokios [...] **tame kontekste** gautos neskelbtinos ar konfidencialios informacijos jokioms trečiosioms šalims. **Tarpusavio mokymosi veikloje dalyvaujanti valstybė narė gali dėl tinkamai pagrįstų priežasčių, apie kurias pranešta Bendradarbiavimo grupei, paprieštarauti tam, kad būtų paskirti konkretūs ekspertai.**

5. Tie patys tarpusavio mokymosi raunde peržiūrėti aspektai ketverius metus po to tarpusavio mokymosi raundo pabaigos toliau neįtraukiami į tarpusavio -[...]mokymosi raundus dalyvaujančių valstybių narių atžvilgiu [...], išskyrus atvejus, kai atitinkama valstybė narė to paprašo arba su tuo sutinka [...] Bendradarbiavimo grupei pateikus pasiūlymą[...].
6. [...]
7. Tarpusavio mokymosi raunduose dalyvaujantys ekspertai parengia per [...] vertinimus nustatytų faktų ir išvadų ataskaitų projektus. Valstybėms narėms leidžiama pateikti pastabas dėl joms skirtų atitinkamų ataskaitų projektų; šios pastabos pridedamos prie ataskaitos. Galutinės ataskaitos pateikiamos Bendradarbiavimo grupei[...]. Valstybės narės gali nuspręsti savo atitinkamas ataskaitas paskelbti viešai.

IV SKYRIUS

Kibernetinio saugumo rizikos valdymas ir pareigos pranešti

I SKIRSNIS

Kibernetinio saugumo rizikos valdymas ir pranešimų teikimas

17 straipsnis

Valdymas

1. Valstybės narės užtikrina, kad esminių ir svarbių subjektų valdymo organai patvirtintų kibernetinio saugumo rizikos valdymo priemones, kurių ėmėsi tie subjektai, siekdami laikytis 18 straipsnio, **prižiūrėtų** jo įgyvendinimą ir **galėtų būti patraukti atsakomybėn** už tai, kad subjektai nesilaiko šiame straipsnyje nustatytų pareigų.

Šios dalies taikymas nedaro poveikio valstybės narės nacionalinės teisės aktams, susijusiems su atsakomybės taisyklėmis viešosiose institucijose, taip pat valstybės tarnautojų ir renkamų bei paskirtų pareigūnų atsakomybe.

2. Valstybės narės užtikrina, kad **iš valdymo organo narių būtų reikalaujama** [...] reguliariai dalyvauti specialiuose mokymuose, kad įgytų pakankamai žinių ir įgūdžių, kad galėtų suprasti ir įvertinti kibernetinio saugumo riziką ir valdymo praktiką bei jos poveikį subjekto veiklai.

Kibernetinio saugumo rizikos valdymo priemonės

- 1a. Šioje direktyvoje taikomas visų rūšių pavojus apimantis požiūris, apimantis tinklų ir informacinių sistemų bei jų fizinės aplinkos apsaugą nuo bet kokių įvykių, kurie galėtų kelti pavojų saugomų, perduodamų ar tvarkomų duomenų arba paslaugų, siūlomų tinklų ir informacinių sistemų arba per jas prieinamų, prieinamumui, autentiškumui, vientisumui ar konfidencialumui.
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 **ir atsižvelgiant į įgyvendinimo sąnaudas**, tomis priemonėmis turi būti užtikrinamas toks tinklų ir informacinių sistemų saugumo lygis, kuris atitinka kylančią riziką. **Vertinant tų priemonių proporcingumą, tinkamai atsižvelgiama į subjekto galimybės patirti riziką laipsnį, jo dydį, incidentų tikimybę ir jų sunkumą. Atsižvelgiant į visuomenei keliamos rizikos lygį ir rūšį įvykus incidentams, kurie daro poveikį esminiems arba svarbiems subjektams, svarbiems subjektams gali būti taikomos ne tokios griežtos kibernetinio saugumo rizikos valdymo priemonės, kokios taikomos esminiems subjektams.**

2. 1 dalyje nurodytos priemonės apima bent:

- a) rizikos analizę ir informacinių sistemų saugumo politiką;
- b) incidentų valdymą (incidentų prevencija, aptikimas, [...] reagavimas į juos **ir padėties atitaisymas po jų**);
- c) veiklos tęstinumą ir krizių valdymą;
- d) tiekimo grandinės saugumą, įskaitant su saugumu susijusius aspektus, susijusius su kiekvieno subjekto ir jo **tiesioginių** tiekėjų ar paslaugų teikėjų, pavyzdžiui, duomenų saugojimo ir tvarkymo paslaugų teikėjų arba valdomų saugumo paslaugų teikėjų, santykiais;
- e) tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumą, įskaitant pažeidžiamumo valdymą ir atskleidimą;
- f) politiką ir procedūras [...], skirtas kibernetinio saugumo rizikos valdymo priemonių veiksmingumui įvertinti;
- g) kriptografijos ir šifravimo naudojimo **politiką**;
- ga) žmogiškųjų išteklių saugumą, prieigos kontrolės politiką ir turto valdymą.**

3. Valstybės narės užtikrina, kad, svarstydami 2 dalies d punkte nurodytas tinkamas priemones, iš subjektų [...] **būtų reikalaujama** atsižvelgti į kiekvieno **tiesioginio** tiekėjo ir paslaugų teikėjo pažeidžiamumą ir į jų tiekėjų ir paslaugų teikėjų produktų bendrą kokybę ir kibernetinio saugumo praktiką, įskaitant jų saugumo plėtojimo procedūras. **Valstybės narės taip pat užtikrina, kad, svarstydami 2 dalies d punkte nurodytas tinkamas priemones, subjektai privalėtų atsižvelgti į pagal 19 straipsnio 1 dalį atliktų suderintų rizikos vertinimų rezultatus.**

4. Valstybės narės užtikrina, kad tais atvejais, kai subjektas nustato, kad atitinkamai jo paslaugos ar užduotys neatitinka 2 dalyje nustatytų reikalavimų, jis nepagrįstai nedelsdamas imtųsi visų būtinų taisomųjų priemonių, kad atitinkama paslauga atitiktų reikalavimus.
5. Komisija gali priimti įgyvendinimo aktus, kuriais nustatomos **šio straipsnio 2 dalyje** nurodytų aspektų techninės ir metodinės specifikacijos, **taip pat, prireikus, sektorių ypatumai.**
Komisija ne vėliau kaip [18 mėnesių po šios direktyvos įsigaliojimo] priima įgyvendinimo aktus, kuriais nustatomos 24 straipsnio 1 dalyje nurodytų subjektų ir I priedo 8 punkte nurodytų patikimumo užtikrinimo paslaugų teikėjų techninės ir metodinės specifikacijos. Tie įgyvendinimo aktai priimami laikantis 37 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros. [...] Rengdama [...] tokius įgyvendinimo aktus, Komisija [...], kiek įmanoma, laikosi tarptautinių ir Europos standartų bei atitinkamų techninių specifikacijų ir pagal 12 straipsnio 4 dalies d punktą keičiasi patarimais su Bendradarbiavimo grupe ir ENISA apie įgyvendinimo akto projektą.
6. [...]

19 straipsnis

ES suderinti ypatingos svarbos tiekimo grandinių rizikos vertinimai

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

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

20 straipsnis

Pareigos pranešti

1. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai nepagrįstai nedelsdami praneštų kompetentingoms institucijoms arba CSIRT pagal 3 ir 4 dalis apie bet koki incidentą, turintį didelį poveikį jų paslaugų teikimui. Kai tinkama, tie subjektai nepagrįstai nedelsdami praneša jų paslaugų gavėjams apie **šiuos** 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. **Dėl paties pranešimo fakto pranešančiojo subjekto atsakomybė nepadidėja.**
2. [...]

Kai taikytina, [...] **esminiai ir svarbūs** 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. Kai tinkama, subjektai taip pat praneša tiems gavėjams apie pačią grėsmę. Dėl **paties** pranešimo **fakto** pranešančiojo subjekto atsakomybė nepadidėja.

3. Incidentas laikomas rimtu, jeigu:
- a) dėl incidento atitinkamas subjektas patyrė arba gali patirti didelių **paslaugų** veiklos sutrikimų arba finansinių nuostolių;
 - b) incidentas paveikė arba gali paveikti kitus fizinius ar juridinius asmenis dėl didelių materialinių arba neturtinių nuostolių.
4. Valstybės narės užtikrina, kad 1 dalyje nurodyto pranešimo tikslais atitinkami subjektai kompetentingoms institucijoms arba CSIRT pateiktų:
- a) nepagrįstai nedelsiant ir bet kuriuo atveju per 24 valandas nuo to laiko, kai sužinoma apie incidentą, – pradinį pranešimą **kaip išankstinį įspėjimą**, kuriame, kai taikoma, nurodoma, ar incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai;
 - b) kompetentingos institucijos arba CSIRT prašymu – tarpinę ataskaitą apie atitinkamus atnaujintus duomenis apie padėtį;
 - c) ne vėliau kaip per vieną mėnesį nuo a punkte nurodyto[...] **pradinio pranešimo** pateikimo – **galutinę** ataskaitą, kurioje pateikiama bent ši informacija:
 - i) išsamus incidento, jo sunkumo ir poveikio aprašymas;
 - ii) grėsmės arba pagrindinės priežasties, dėl kurios incidentas galėjo būti sukeltas, rūšį;
 - iii) taikomos ir įgyvendinamos poveikio mažinimo priemonės.

Valstybės narės nustato, kad tinkamai pagrįstais atvejais ir susitarus su kompetentingomis institucijomis arba CSIRT atitinkamas subjektas gali nukrypti nuo a ir c punktuose nustatytų terminų. **Visų pirma nukrypimas nuo c punkte nurodyto termino gali būti pateisinamas tais atvejais, kai incidentas tebesitęsia.**

5. Kompetentingos nacionalinės institucijos arba CSIRT gavusios 4 dalies a punkte nurodytą pradinį pranešimą [...] **nepagrįstai nedelsdamos** pateikia atsakymą pranešančiajam subjektui, įskaitant pirminę grįžtamąją informaciją apie incidentą, o subjekto prašymu – galimų rizikos mažinimo priemonių įgyvendinimo gaires. Jei CSIRT negavo 1 dalyje nurodyto pranešimo, gaires teikia kompetentinga institucija, bendradarbiaudama su CSIRT. CSIRT teikia papildomą techninę pagalbą, jei to prašo atitinkamas subjektas. Jei įtariama, kad incidentas yra baudžiamojo pobūdžio, kompetentingos nacionalinės institucijos arba CSIRT taip pat teikia gaires dėl pranešimo apie incidentą teisėsaugos institucijoms.
6. Kai tikslinga ir visų pirma tuomet, kai 1 dalyje nurodytas incidentas yra susijęs su dviem ar daugiau valstybių narių, kompetentinga institucija, CSIRT arba **bendrasis informacinis centras** apie incidentą informuoja kitas paveiktas valstybes nares ir ENISA. **Tokia informacija apima bent šio straipsnio 4 dalyje nurodytus elementus.** Tai darydamos kompetentingos institucijos, CSIRT ir bendrieji informaciniai centrai pagal Sąjungos teisę arba Sąjungos teisę atitinkančius nacionalinės teisės aktus saugo subjekto saugumo ir komercinius interesus, taip pat pateiktos informacijos konfidencialumą.
7. Kai visuomenės informuotumas yra būtinas siekiant užkirsti kelią incidentui ar reaguoti į besitęsiantį incidentą arba kai incidento atskleidimas kitais atvejais atitinka viešąjį interesą, kompetentinga institucija arba CSIRT ir, kai tikslingas, kitų atitinkamų valstybių narių institucijos arba CSIRT, pasikonsultavusios su atitinkamu subjektu, gali informuoti visuomenę apie incidentą arba pareikalauti, kad tai padarytų subjektas.

8. Kompetentingos institucijos arba CSIRT prašymu bendrasis informacinis centras perduoda pagal 1 [...] dalį gautus pranešimus kitų paveiktų valstybių narių bendriesiems informaciniams centrams.
9. Bendrasis informacinis centras kas [...] **šešis mėnesius** 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. **ENISA kas šešis mėnesius informuoja Bendradarbiavimo grupę ir CSIRT tinklą apie savo išvadas dėl gautų pranešimų.**
10. Kompetentingos institucijos pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva] paskirtoms kompetentingoms institucijoms teikia informaciją apie incidentus ir kibernetines grėsmes, apie kuriuos pagal 1 ir 2 dalis pranešė esminiai subjektai, nustatyti kaip ypatingos svarbos subjektai [arba ypatingos svarbos subjektams lygiaverčiai subjektai] pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva].
11. Komisija gali priimti įgyvendinimo aktus, kuriais išsamiau nustatoma pagal 1 ir 2 dalis pateikto pranešimo rūšis, formatas ir procedūra. Komisija taip pat gali priimti įgyvendinimo aktus, kuriais išsamiau nustatomi atvejai, kuriais incidentas laikomas rimtu, kaip nurodyta 3 dalyje. Tie įgyvendinimo aktai priimami laikantis 37 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

Europos kibernetinio saugumo sertifikavimo schemų naudojimas

1. Siekdamos įrodyti atitiktį tam tikriems 18 straipsnio reikalavimams, **valstybės narės gali reikalauti, kad subjektai naudotų tam tikrus IRT produktus, [...] paslaugas ir [...] procesus, sertifikuotus** pagal konkrečias Europos kibernetinio saugumo sertifikavimo schemas, priimtas pagal Reglamento (ES) 2019/881 49 straipsnį. Sertifikuojamus **IRT produktus, paslaugas ir procesus** gali kurti esminis arba svarbus subjektas arba jie gali būti perkami iš trečiųjų šalių.
2. Komisija gali [...] priimti [...] **įgyvendinimo** aktus, kuriais nustatoma, kokių kategorijų esminiams **ar svarbiems** subjektams reikia **naudoti tam tikrus sertifikuotus IRT produktus, paslaugas ir procesus arba** gauti sertifikatą, [...] pagal kurias [...] Europos kibernetinio saugumo sertifikavimo schemas, **priimtas pagal Reglamento (ES) 2019/881 49 straipsnį. Tie įgyvendinimo aktai priimami laikantis 37 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros. Rengdama tokius įgyvendinimo aktus, Komisija, vadovaudamasi Reglamento (ES) 2019/881 56 straipsniu:**
 - i) **atsižvelgia į tokių priemonių poveikį tokių IRT produktų gamintojams, paslaugų teikėjams ar procesų vykdytojams ir jų naudotojams, kiek tai susiję su tų priemonių sąnaudomis ir visuomenine ar ekonomine nauda dėl numatomo didesnio saugumo užtikrinimo tiksliniams IRT produktams, paslaugoms ar procesams, taip pat dėl jų alternatyvų prieinamumo rinkoje;**
 - ii) **vykdo atvirą, skaidrų ir įtraukų konsultavimosi procesą su visais atitinkamais suinteresuotaisiais subjektais ir valstybėmis narėmis;**

- (i) **atsižvelgia į įgyvendinimo terminus, pereinamojo laikotarpio priemones ir laikotarpius, visų pirma dėl galimo priemonių poveikio IRT produktų gamintojams, paslaugų teikėjams ar procesų vykdytojams arba jų naudotojams, ypač MVĮ;**
- (ii) **atsižvelgia į atitinkamų valstybių narių teisės aktų buvimą ir įgyvendinimą.**

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

22 straipsnis

Standartizacija

1. Siekdamas skatinti vienodą 18 straipsnio 1 ir 2 dalių įgyvendinimą, valstybės narės, nereikalaudamos taikyti kokios nors konkrečios rūšies technologijos ir nesuteikdamos jai pirmenybės, skatina naudotis europiniais ar tarptautiniu mastu pripažintais standartais ir specifikacijomis, kurie yra svarbūs tinklų ir informacinių sistemų saugumui.
2. ENISA, bendradarbiaudama su valstybėmis narėmis, parengia rekomendacijas ir gaires dėl techninių sričių, kurios turi būti apsvarstytos atsižvelgiant į 1 dalį, taip pat dėl jau galiojančių standartų, be kita ko, valstybių narių nacionalinių standartų, kuriuose būtų numatyta įtraukti tas sritis.

Domenų vardų ir registracijos duomenų bazės

1. Siekdamos prisidėti prie DNS saugumo, stabilumo ir atsparumo, valstybės narės užtikrina, kad aukščiausio lygio domenų vardų registrai ir aukščiausio lygio domenų atveju domenų vardų registravimo paslaugas teikiantys subjektai su deramu stropumu rinktų ir specialioje duomenų bazėje saugotų tikslus, [...] ir išsamius domenų vardų registracijos duomenis, **laikydami** [...] Sąjungos duomenų apsaugos teisės dėl duomenų, kurie yra asmens duomenys.
2. Valstybės narės užtikrina, kad 1 dalyje nurodytose domenų vardų registracijos duomenų bazėse būtų atitinkama informacija, pagal kurią būtų galima nustatyti domenų vardų turėtojus ir kontaktinius centrus, administruojančius aukščiausio lygio domenų vardais pažymėtus domenų vardus, ir su jais susisiekti, **įskaitant bent šiuos duomenis:**
 - a) **domeno vardą,**
 - b) **registracijos datą,**
 - c) **registruotojo duomenis, įskaitant:**
 - i) **fizinių asmenų atveju – vardą, pavardę ir el. pašto adresą;**
 - ii) **juridinių asmenų atveju – pavadinimą ir el. pašto adresą.**

3. Valstybės narės užtikrina, kad aukščiausio lygio domenų vardų registrai ir aukščiausio lygio domenų atveju domenų vardų registravimo paslaugas teikiantys subjektai taikytų politiką ir procedūras, kuriomis užtikrinama, kad duomenų bazėse būtų pateikiama tiksli ir išsami informacija. Valstybės narės užtikrina, kad tokia politika ir procedūros būtų skelbiamos viešai.
4. Valstybės narės užtikrina, kad aukščiausio lygio domenų vardų registrai ir aukščiausio lygio domenų atveju domenų vardų registravimo paslaugas teikiantys subjektai nepagrįstai nedelsdami po domeno vardo užregistravimo paskelbtų domeno registracijos duomenis, kurie nėra asmens duomenys.
5. Valstybės narės užtikrina, kad aukščiausio lygio domenų vardų registrai ir aukščiausio lygio domenų atveju domenų vardų registravimo paslaugas teikiantys subjektai, 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 aukščiausio lygio domenų atveju domenų vardų registravimo paslaugas teikiantys subjektai nepagrįstai nedelsdami **ir bet kuriuo atveju per 72 valandas** atsakytų į visus prašymus suteikti prieigą. Valstybės narės užtikrina, kad tokių duomenų atskleidimo politika ir procedūros būtų skelbiamos viešai.

Jurisdikcija ir registracija

24 straipsnis

Jurisdikcija ir teritoriškumas

- 1a. Laikoma, kad subjektai pagal šią direktyvą priklauso valstybės narės, kurioje jie teikia paslaugas, jurisdikcijai. Laikoma, kad I priedo 1–7 ir 10 punktuose nurodyti subjektai, I priedo 8 punkte nurodyti patikimumo užtikrinimo paslaugų teikėjai ir interneto duomenų srautų mainų taško teikėjai ir II priedo 1–5 punktuose nurodyti subjektai priklauso valstybės narės, kurioje jie yra įsisteigę, jurisdikcijai.**
1. DNS paslaugų teikėjai, aukščiausio lygio domenų vardų registrai [...] **ir aukščiausio lygio domenų atveju domenų vardų registravimo paslaugas teikiantys subjektai**, debesijos kompiuterijos paslaugų teikėjai, duomenų centrų paslaugų teikėjai, [...] turinio teikimo tinklo paslaugų teikėjai, **valdomų paslaugų teikėjai ir valdomų saugumo paslaugų teikėjai**, nurodyti I priedo 8 ir **8a punktuose**, taip pat II priedo 6 punkte nurodyti skaitmeninių paslaugų teikėjai laikomi priklausančiais valstybės narės, kurioje yra jų pagrindinė buveinė Sąjungoje, jurisdikcijai.
2. Taikant šią direktyvą laikoma, kad 1 dalyje nurodytų subjektų pagrindinė buveinė Sąjungoje yra valstybėje narėje, kurioje **daugiausia** priimami su kibernetinio saugumo rizikos valdymo priemonėmis susiję sprendimai. Jei **vieta, kurioje tokie sprendimai daugiausia priimami, negali būti nustatyta, arba** tokie sprendimai nepriimami jokiame padalinyje Sąjungoje, laikoma, kad pagrindinė buveinė yra valstybėje narėje, kurioje subjektas turi padalinį, kuriame dirba daugiausia darbuotojų Sąjungoje. **Jeigu paslaugas teikia įmonių grupė, pagrindine buveine laikoma pagrindinė įmonių grupės buveinė.**

3. Jei 1 dalyje nurodytas subjektas nėra įsisteigęs Sąjungoje, bet teikia paslaugas Sąjungoje, jis paskiria atstovą Sąjungoje. Atstovas turi būti įsisteigęs vienoje iš tų valstybių narių, kuriose teikiamos paslaugos. Laikoma, kad toks subjektas priklauso valstybės narės, kurioje yra įsisteigęs jo atstovas, jurisdikcijai. Jei pagal šį straipsnį Sąjungoje nėra paskirto atstovo, bet kuri valstybė narė, kurioje subjektas teikia paslaugas, gali imtis teisinių veiksmų prieš subjektą dėl šioje direktyvoje nustatytų pareigų nevykdymo.
4. 1 dalyje nurodyto subjekto atstovo paskyrimas nedaro poveikio teisiniams veiksams, kurie galėtų būti inicijuoti prieš patį subjektą.
- 4a. **Valstybės narės, gavusios savitarpio pagalbos prašymą dėl 1 dalyje nurodytų subjektų, gali, neviršydamos prašymo ribų, imtis tinkamų priežiūros ir vykdymo užtikrinimo priemonių, susijusių su atitinkamu subjektu, teikiančiu paslaugas arba turinčiu tinklų ir informacinę sistemą jų teritorijoje.**

25 straipsnis

Tam tikrų skaitmeninės infrastruktūros subjektų ir skaitmeninių paslaugų teikėjų registras

1. [...] Valstybės narės užtikrina, kad [...] 24 straipsnio 1 dalyje nurodytiems subjektams, kurių pagrindinė buveinė yra jų teritorijoje arba kurių, jeigu jie nėra įsisteigę Sąjungoje, paskirtas atstovas Sąjungoje yra įsisteigęs jų teritorijoje, būtų nustatytas reikalavimas ne vėliau kaip [ne daugiau kaip 12 mėnesių po direktyvos įsigaliojimo] pateikti kompetentingoms institucijoms šią informaciją:

- a) subjekto pavadinimą;
- aa) subjekto rūšį pagal šios direktyvos I ir II priedus;**
- b) savo pagrindinės buveinės adresą ir kitus juridinius padalinius Sąjungoje arba, jei jie nėra įsisteigę Sąjungoje, pagal 24 straipsnio 3 dalį paskirto atstovo adresą;
- c) naujausius kontaktinius duomenis, įskaitant subjektų **ir jų atstovų** e. pašto adresus ir telefono numerius;
- d) valstybes nares, kuriose subjektas teikia paslaugą.**

Kai taikytina, ši informacija pateikiama per 2a straipsnyje nurodytą nacionalinį [...] pranešimo apie save mechanizmą.

- 2. **Valstybės narės užtikrina, kad [...] 1 dalyje nurodyti subjektai taip pat praneštų [...] apie bet kokius pagal 1 dalį pateiktos informacijos pakeitimus nedelsdami ir bet kuriuo atveju ne vėliau kaip per tris mėnesius nuo pakeitimo įsigaliojimo dienos.**
- 3. **[...] Valstybių narių bendrieji informaciniai centrai perduoda 1 ir 2 dalyse nurodytą informaciją [...] [...] ENISA. [...]**

3a. Remdamasi informacija, gauta pagal šio straipsnio 3 dalį, ENISA sukuria ir tvarko 1 dalyje nurodytų subjektų registrą. Valstybių narių prašymu ENISA suteikia atitinkamoms kompetentingoms institucijoms prieigą prie registro, kartu, kai taikytina, užtikrindama būtiną informacijos konfidencialumo apsaugos garantijas.

4. [...]

V SKYRIUS

Dalijimasis informacija

26 straipsnis

Dalijimosi kibernetinio saugumo informacija susitarimai

1. [...] Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai galėtų **savanoriškai** tarpusavyje keistis svarbia kibernetinio saugumo informacija, įskaitant informaciją, susijusią su kibernetinėmis grėsmėmis, **vos neįvykusiais incidentais**, pažeidžiamumu, užvaldymo rodikliais, taktika, metodais ir procedūromis, kibernetinio saugumo perspėjimais ir konfigūracijos priemonėmis, kai tokiu dalijimusi informacija:
 - a) siekiama užkirsti kelią incidentams, juos nustatyti, į juos reaguoti arba juos sušvelninti;

- b) didinamas kibernetinis saugumas, visų pirma didinant informuotumą apie kibernetines grėsmes, ribojant arba trukdant tokioms grėsmėms plisti, remiant įvairius gynybos pajėgumus, pažeidžiamumo ištaisymą ir atskleidimą, grėsmių nustatymo metodus, švelninimo strategijas arba reagavimo ir atsigavimo etapus.
2. Valstybės narės užtikrina, kad informacija būtų keičiamasi [...] esminių ir svarbių subjektų bendruomenėse. Toks keitimasis vykdomas taikant dalijimosi informacija susitarimus, susijusius su galimai neskelbtina informacija, kuria keičiamasi [...].
3. Valstybės narės **gali** [...] nustatyti taisykles, kuriose aprašoma 2 dalyje nurodytų dalijimosi informacija susitarimų procedūra, veiklos elementai (įskaitant specialią IRT platformų naudojimą), turinys ir sąlygos. Tokiose taisyklėse taip pat **gali būti** [...] nustatyta išsami informacija apie valdžios institucijų dalyvavimą tokiuose susitarimuose, taip pat veiklos elementai, įskaitant specialią IT platformų naudojimą. Valstybės narės teikia paramą tokių priemonių taikymui pagal 5 straipsnio 2 dalies g punkte nurodytą savo politiką.
4. Esminiai ir svarbūs subjektai kompetentingoms institucijoms praneša apie savo dalyvavimą 2 dalyje nurodytuose dalijimosi informacija susitarimuose jiems įsigaliojus arba, kai tinkama, apie pasitraukimą iš tokių susitarimų, kai toks pasitraukimas įsigalioja.
5. [...] ENISA remia 2 dalyje nurodytų dalijimosi kibernetinio saugumo informacija susitarimų sudarymą, teikdama geriausios praktikos pavyzdžius ir gaires.

Savanoriškas pranešimas apie svarbią informaciją

1. **Nedarant poveikio 20 straipsniui, valstybės narės užtikrina, kad esminiai ir svarbūs subjektai galėtų savanoriškai pranešti kompetentingoms institucijoms arba CSIRT apie visus atitinkamus incidentus, kibernetines grėsmes arba vos neįvykusius incidentus.**
2. 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. **Nedarant poveikio nusikalstamų veikų tyrimui, jų atskleidimui ir baudžiamajam persekiojimui už jas, [...]** dėl savanoriško pranešimo pranešančiajam subjektui nenustatoma jokių papildomų pareigų, kurios jam nebūtų taikomos, jei jis nebūtų pateikęs pranešimo.
3. **Savanoriški pranešimai tvarkomi tik tuo atveju, jei dėl tokio tvarkymo atitinkamoms valstybėms narėms nesusidaro neproporcinga arba netinkama našta.**

VI SKYRIUS

Priežiūra ir vykdymo užtikrinimas

28 straipsnis

Bendrieji aspektai, susiję su priežiūra ir vykdymo užtikrinimu

1. Valstybės narės užtikrina, kad kompetentingos institucijos veiksmingai vykdytų stebėseną ir imtųsi priemonių, būtinų užtikrinti, kad būtų laikomasi šios direktyvos [...], visų pirma 18, [...], 20 ir 23 straipsniuose nustatytų pareigų. **Valstybės narės gali leisti kompetentingoms institucijoms teikti pirmenybę priežiūrai, kuri turi būti grindžiama rizika grindžiamu požyriu.**
2. Kompetentingos institucijos, nagrinėdamos kibernetinio saugumo incidentus [...], glaudžiai bendradarbiauja su duomenų apsaugos institucijomis, **kompetentingomis institucijomis, paskirtomis pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva], priežiūros įstaigomis, paskirtoms pagal Reglamentą (ES) 910/2014, ir kitomis kompetentingomis institucijomis, paskirtomis pagal konkrečius sektoriams taikomus Sąjungos teisės aktus.**
3. **Nedarant poveikio nacionalinėms teisėkūros ir institucinėms sistemoms, valstybės narės užtikrina, kad, vykdydamos priežiūrą, kaip viešojo administravimo subjektai laikosi šios direktyvos, ir užtikrindamos galimų sankcijų už nesilaikymą vykdymą, kompetentingos institucijos turėtų atitinkamus įgaliojimus vykdyti tokias užduotis turėdamos veiklos nepriklausomumą nuo prižiūrimų subjektų. Valstybės narės gali nuspręsti dėl tinkamų, proporcingų ir veiksmingų priežiūros ir vykdymo užtikrinimo priemonių nustatymo šių subjektų atžvilgiu pagal nacionalines sistemas ir teisinę tvarką.**

Esminių subjektų priežiūra ir vykdymo užtikrinimas

1. Valstybės narės užtikrina, kad priežiūros ar vykdymo užtikrinimo priemonės, taikomos svarbiausiems subjektams vykdant šioje direktyvoje nustatytas pareigas, būtų veiksmingos, proporcingos ir atgrasomos, atsižvelgiant į kiekvieno atskiro atvejo aplinkybes.
2. Valstybės narės užtikrina, kad kompetentingos institucijos, vykdydamos savo priežiūros užduotis, susijusias su esminiais subjektais, **laikytusi rizika grindžiamo požiūrio ir turėtų bent tokius** įgaliojimus dėl tų subjektų:
 - a) atlikti patikrinimus vietoje ir priežiūrą ne vietoje, įskaitant atsitiktinius patikrinimus;
 - b) atlikti reguliarius **saugumo** auditus;
 - c) atlikti tikslingus saugumo auditus, pagrįstus rizikos vertinimais arba prieinama informacija apie riziką;
 - d) atlikti saugumo patikrinimus, pagrįstus objektyviais, nediskriminaciniais, sąžiningais ir skaidriais rizikos vertinimo kriterijais, **bendradarbiaudamos, kai to reikia dėl techninių priežasčių, su atitinkamu subjektu**;
 - e) prašyti pateikti informaciją, būtiną subjekto priimtoms kibernetinio saugumo priemonėms įvertinti, įskaitant dokumentais pagrįstą kibernetinio saugumo politiką [...];
 - f) prašyti leisti susipažinti su duomenimis, dokumentais ar bet kokia informacija, reikalinga jų priežiūros užduotims atlikti;
 - g) prašyti pateikti kibernetinio saugumo politikos įgyvendinimo įrodymus, pavyzdžiui, kvalifikuoto auditoriaus atliktų saugumo auditų rezultatus ir atitinkamus pagrindinius įrodymus.

- 2a. Vykdydamos savo priežiūros užduotis, numatytas šio straipsnio 2 dalyje, kompetentingos institucijos gali nustatyti priežiūros metodikas, pagal kurias galima būtų nustatyti tokių užduočių prioritetus, laikantis rizika grindžiamo požiūrio.
3. Naudodamosi savo įgaliojimais pagal 2 dalies e–g punktus, kompetentingos institucijos nurodo prašymo tikslą ir prašomą informaciją.
4. Valstybės narės užtikrina, kad kompetentingos institucijos, naudodamosi savo vykdymo užtikrinimo įgaliojimais esminių subjektų atžvilgiu, turėtų **bent tokius** įgaliojimus:
- a) įspėti, kad subjektai nesilaiko šioje direktyvoje nustatytų pareigų;
 - b) priimti privalomus nurodymus arba įsakymą, kuriuo reikalaujama, kad tie subjektai pašalintų nustatytus trūkumus arba šioje direktyvoje nustatytų pareigų pažeidimus;
 - c) nurodyti tiems subjektams nutraukti veiksmus, kurie neatitinka šioje direktyvoje nustatytų pareigų, ir nebekartoti tokių veiksmų;
 - d) nurodyti tiems subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų rizikos valdymo priemonės ir (arba) pareigos pranešti atitiktų 18 ir 20 straipsniuose nustatytas pareigas;
 - e) nurodyti tiems subjektams informuoti fizinį (-ius) arba juridinį (-ius) asmenį (-is), kuriam (-iems) jie teikia paslaugas arba vykdo veiklą, kurioms gali pakenkti didelė kibernetinė grėsmė, **apie grėsmės pobūdį, taip pat** apie visas galimas apsaugos ar taisomąsias priemones, kurių gali imtis tas (tie) fizinis (-iai) ar juridinis (-iai) asmuo (-enys), reaguodamas (-i) į tą grėsmę;
 - f) nurodyti tiems subjektams per pagrįstą terminą įgyvendinti saugumo audito metu pateiktas rekomendacijas;
 - g) [...]

h) nurodyti tiems subjektams konkrečiu būdu viešai paskelbti šioje direktyvoje nustatytų pareigų nevykdymo aspektus, **jei dėl tokio viešo atskleidimo atitinkamas subjektas nepatirtų žalingo poveikio**;

i) [...]

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

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

a) sustabdyti arba prašyti, kad sertifikavimo arba leidimus išduodanti įstaiga **ar teismai pagal nacionalinės teisės aktus** sustabdytų sertifikavimą arba įgaliojimą, susijusį su dalimi arba visomis esminės įstaigos teikiamomis paslaugomis ar veikla;

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

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

Šioje dalyje nurodytos sankcijos netaikomos viešojo administravimo subjektams, kuriems taikoma ši direktyva.

6. Valstybės narės užtikrina, kad bet kuris fizinis asmuo, atsakingas už esminį subjektą arba veikiantis kaip jo atstovas, remdamasis jam suteiktais įgaliojimais, įgaliojimu priimti sprendimus jo vardu arba įgaliojimu vykdyti jo kontrolę, turėtų įgaliojimus užtikrinti, kad jis laikytųsi šioje direktyvoje nustatytų pareigų. Valstybės narės užtikrina, kad tie fiziniai asmenys galėtų būti traukiami atsakomybėn už jų pareigų užtikrinti šioje direktyvoje nustatytų pareigų vykdymą pažeidimą. **Viešojo administravimo subjektų atžvilgiu šia nuostata nedaromas poveikis valstybių narių teisės aktams, susijusiems su valstybės tarnautojų ir renkamų bei paskirtų pareigūnų atsakomybe.**
7. Imdamosi kokių nors vykdymo užtikrinimo veiksmų arba taikydamos sankcijas pagal 4 ir 5 dalis, kompetentingos institucijos gerbia teisę į gynybą ir atsižvelgia į kiekvieno atskiro atvejo aplinkybes ir tinkamai atsižvelgia bent į:
 - a) pažeidimo sunkumą ir pažeistų nuostatų svarbą. Pažeidimai, kurie turėtų būti laikomi sunkiais: pakartotiniai pažeidimai, nepranešimas apie incidentus, turinčius didelį trikdantį poveikį, ir negebėjimas jų išspręsti, negebėjimas ištaisyti trūkumų pagal kompetentingų institucijų privalomus nurodymus, trukdymas vykdyti audito ar stebėsenos veiklą, kurią nurodė atlikti kompetentinga institucija po to, kai buvo nustatytas pažeidimas, neteisingos ar labai netikslios informacijos, susijusios su 18 ir 20 straipsniuose nustatytais rizikos valdymo reikalavimais arba pareigomis pranešti, pateikimas;

- b) pažeidimo trukmę, įskaitant pakartotinių pažeidimų elementą;
 - c) faktiškai padarytą žalą ar patirtus nuostolius arba galimą žalą ar nuostolius, kurie galėjo būti patirti, jei juos galima nustatyti. Vertinant šį aspektą, be kita ko, atsižvelgiama į faktinius ar galimus finansinius ar ekonominius nuostolius, poveikį kitoms paslaugoms, paveiktų ar galimai paveiktų naudotojų skaičių;
 - d) tai, ar pažeidimas padarytas tyčia, ar dėl aplaidumo;
 - e) priemonės, kurių subjektas ėmėsi siekdamas užkirsti kelią žalai ir (arba) nuostoliams arba juos sumažinti;
 - f) patvirtintų elgesio kodeksų arba patvirtintų sertifikavimo mechanizmų laikymąsi;
 - g) atsakingu (-ais) laikomo (-ų) fizinio (-ų) ar juridinio (-ų) asmens (-ų) bendradarbiavimo su kompetentingomis institucijomis lygį.
8. Kompetentingos institucijos išsamiai pagrindžia savo vykdymo užtikrinimo sprendimus. Prieš priimdamos tokius sprendimus kompetentingos institucijos atitinkamiems subjektams praneša savo preliminarį išvadą ir suteikia tiems subjektams pagrįstą laikotarpį pastaboms pateikti, **išskyrus gresiančio pavojaus atvejus.**

9. Valstybės narės užtikrina, kad jų **pagal šią direktyvą** kompetentingos institucijos informuotų atitinkamas [...] **tos pačios** 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. **Kai tikslinga**, [...] pagal Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva] kompetentingos institucijos [...] **gali paprašyti pagal šią direktyvą** [...] kompetentingų institucijų naudotis savo priežiūros ir vykdymo užtikrinimo **įgaliojimais** esminio subjekto, kuriam taikoma ši direktyva ir kuris taip pat laikomas ypatingos svarbos subjektu pagal **Direktyvą (ES) XXXX/XXXX [Ypatingos svarbos subjektų atsparumo direktyva]** [arba jam lygiaverčiu], atžvilgiu.
10. Valstybės narės užtikrina, kad jų pagal šią direktyvą kompetentingos institucijos informuotų Priežiūros forumą pagal Reglamento (ES) XXXX/XXXX [DORA] 29 straipsnio 1 dalį, kai jos naudojasi priežiūros ir vykdymo užtikrinimo įgaliojimais, kuriais siekiama užtikrinti, kad esminis subjektas, paskirtas ypatingos svarbos IRT paslaugas teikiančia trečiaja šalimi pagal Reglamento (ES) XXXX/XXXX [DORA] 28 straipsnį, laikytųsi šioje direktyvoje nustatytų pareigų.
- 10a. Valstybės narės užtikrina, kad jų pagal šią direktyvą kompetentingos institucijos informuotų atitinkamas kompetentingas institucijas, paskirtas pagal Reglamentą (ES) Nr. 910/2014, kai jos naudojasi priežiūros ir vykdymo užtikrinimo įgaliojimais, kuriais siekiama užtikrinti, kad subjektas, paskirtas patikimumo užtikrinimo paslaugų teikėju pagal Reglamentą (ES) Nr. 910/2014, laikytųsi šioje direktyvoje nustatytų pareigų.

Svarbių subjektų priežiūra ir vykdymo užtikrinimas

1. Gavusios įrodymų, nuorodų **ar informacijos**, kad svarbus subjektas, **kaip įtariama**, nesilaiko šioje direktyvoje, visų pirma 18 ir 20 straipsniuose, nustatytų pareigų, valstybės narės užtikrina, kad kompetentingos institucijos prireikus imtųsi veiksmų taikydamos *ex post* priežiūros priemonės.
2. Valstybės narės užtikrina, kad kompetentingos institucijos, vykdydamos savo priežiūros užduotis, susijusias su svarbiais subjektais, **laikytųsi rizika grindžiamo požiūrio ir turėtų bent tokius** įgaliojimus dėl tų subjektų:
 - a) atlikti patikrinimus vietoje ir vykdyti *ex post* priežiūrą ne vietoje;
 - b) atlikti tikslingus saugumo auditus, pagrįstus rizikos vertinimais arba prieinama informacija apie riziką;
 - c) atlikti saugumo patikrinimus, pagrįstus objektyviais, **nediskriminaciniais**, sąžiningais ir skaidriais rizikos vertinimo kriterijais, **bendradarbiaudamos, kai to reikia dėl techninių priežasčių, su atitinkamu subjektu**;
 - d) prašyti pateikti bet kokią informaciją, būtiną subjekto kibernetinio saugumo priemonėms *ex post* įvertinti [...];
 - e) prašyti leisti susipažinti su duomenimis, dokumentais ir (arba) bet kokia informacija, reikalinga priežiūros užduotims atlikti;
 - ea) **prašyti pateikti kibernetinio saugumo politikos įgyvendinimo įrodymus, pavyzdžiui, kvalifikuoto auditoriaus atliktų saugumo auditų rezultatus ir atitinkamus pagrindinius įrodymus.**

- 2a. Vykdydamos savo priežiūros užduotis, numatytas šio straipsnio 2 dalyje, kompetentingos institucijos gali nustatyti priežiūros metodikas, pagal kurias galima būtų nustatyti tokių užduočių prioritetus, laikantis rizika grindžiamo požiūrio.
3. Naudodamosi savo įgaliojimais pagal 2 dalies d–ea punktus, kompetentingos institucijos nurodo prašymo tikslą ir patikslina prašomą informaciją.
4. Valstybės narės užtikrina, kad kompetentingos institucijos, naudodamosi savo vykdymo užtikrinimo įgaliojimais svarbių subjektų atžvilgiu, turėtų **bent tokius** įgaliojimus:
- a) įspėti, kad subjektai nesilaiko šioje direktyvoje nustatytų pareigų;
 - b) priimti privalomus nurodymus arba įsakymą, kuriuo reikalaujama, kad tie subjektai pašalintų nustatytus trūkumus arba šioje direktyvoje nustatytų pareigų pažeidimą;
 - c) nurodyti tiems subjektams nutraukti veiksmus, kurie neatitinka šioje direktyvoje nustatytų pareigų, ir nebekartoti tokių veiksmų;
 - d) nurodyti tiems subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų rizikos valdymo priemonės arba pareigos pranešti atitiktų 18 ir 20 straipsniuose nustatytas pareigas;
 - e) nurodyti tiems subjektams informuoti fizinį (-ius) arba juridinį (-ius) asmenį (-is), kuriam (-iems) jie teikia paslaugas arba vykdo veiklą, kurioms gali pakenkti didelė kibernetinė grėsmė, **apie grėsmės pobūdį, taip pat** apie visas galimas apsaugos ar taisomąsias priemones, kurių gali imtis tas (tie) fizinis (-iai) ar juridinis (-iai) asmuo (-enys), reaguodamas (-i) į tą grėsmę;
 - f) nurodyti tiems subjektams per pagrįstą terminą įgyvendinti saugumo audito metu pateiktas rekomendacijas;

- g) nurodyti tiems subjektams konkrečiu būdu viešai paskelbti šioje direktyvoje nustatytų jų pareigų nevykdymo aspektus, **jei dėl tokio viešo atskleidimo atitinkamas subjektas nepatirtų žalingo poveikio**;
 - h) [...]
 - i) skirti arba prašyti, kad atitinkamos įstaigos ar teismai pagal nacionalinės teisės aktus skirtų administracinę baudą pagal 31 straipsnį, kartu su šios dalies a–h punktuose nurodytomis priemonėmis arba vietoj jų, atsižvelgiant į kiekvieno atskiro atvejo aplinkybes.
5. 29 straipsnio 6–8 dalys taip pat taikomos šiame straipsnyje numatytoms priežiūros ir vykdymo užtikrinimo priemonėms, skirtoms [...] svarbiems subjektams.

31 straipsnis

Bendrosios administracinių baudų skyrimo esminiams ir svarbiems subjektams sąlygos

1. Valstybės narės užtikrina, kad už šioje direktyvoje nustatytų pareigų pažeidimus esminiams ir svarbiems subjektams skiriamos administracinės baudos pagal šį straipsnį kiekvienu atskiru atveju būtų veiksmingos, proporcingos ir atgrasomos.
2. Administracinės baudos, atsižvelgiant į kiekvieno atskiro atvejo aplinkybes, skiriamos kartu su 29 straipsnio 4 dalies a–i punktuose, 29 straipsnio 5 dalyje ir 30 straipsnio 4 dalies a–h punktuose nurodytomis priemonėmis arba vietoj jų.
3. Sprendžiant, ar skirti administracinę baudą, ir kiekvienu atskiru atveju priimant sprendimą dėl jos dydžio, deramai atsižvelgiama bent į 29 straipsnio 7 dalyje nurodytus aspektus.

4. Valstybės narės užtikrina, kad **esminiams subjektams** už 18 arba 20 straipsnyje nustatytų pareigų pažeidimus pagal šio straipsnio 2 ir 3 dalis būtų skiriamos administracinės baudos, kurių didžiausia suma būtų ne mažesnė kaip 4 000 000 EUR arba, **juridinio asmens atveju**, [...] 2 proc. įmonės, kuriai tas esminis [...] subjektas priklauso, bendros pasaulinės metinės apyvartos praėjusiais finansiniais metais, atsižvelgiant į tai, kuri suma yra didesnė.
- 4a. Valstybės narės užtikrina, kad svarbiems subjektams už 18 arba 20 straipsnyje nustatytų pareigų pažeidimus pagal šio straipsnio 2 ir 3 dalis būtų skiriamos administracinės baudos, kurių didžiausia suma būtų ne mažesnė kaip 2 000 000 EUR arba, juridinio asmens atveju, 1 proc. įmonės, kuriai tas svarbus subjektas priklauso, bendros pasaulinės metinės apyvartos praėjusiais finansiniais metais, atsižvelgiant į tai, kuri suma yra didesnė.**
5. Valstybės narės gali numatyti įgaliojimą skirti periodines baudas, siekiant priversti esminį arba svarbų subjektą nutraukti pažeidimą, remiantis išankstiniu kompetentingos institucijos sprendimu.
6. Nedarant poveikio kompetentingų institucijų įgaliojimams pagal 29 ir 30 straipsnius, kiekviena valstybė narė gali nustatyti taisykles dėl to, ar ir koku mastu administracinės baudos gali būti skiriamos 4 straipsnio 23 dalyje nurodytiems viešojo administravimo subjektams, atsižvelgiant į šioje direktyvoje nustatytas pareigas.

- 6a. Jei valstybės narės teisės sistemoje nenumatoma administracinių baudų, valstybės narės užtikrina, kad šis straipsnis galėtų būti taikomas taip, kad baudą inicijuotų kompetentinga institucija, o ją skirtų kompetentingi nacionaliniai teismai, kartu užtikrinant, kad tos teisių gynimo priemonės būtų veiksmingos ir turėtų kompetentingų institucijų skiriamoms administracinėms baudoms lygiavertį poveikį. Bet kuriuo atveju skiriamos baudos turi būti veiksmingos, proporcingos ir atgrasomos. Tos valstybės narės ne vėliau kaip [...] praneša Komisijai savo teisės aktų nuostatas, kurias jos priima pagal šią dalį, ir nedelsdamos praneša apie vėlesnius tas nuostatas keičiančius teisės aktus ar su jomis susijusius pakeitimus.

32 straipsnis

Pažeidimai, susiję su asmens duomenų saugumo pažeidimu

1. Jeigu, vykdydamos priežiūrą ar vykdymo užtikrinimą, kompetentingos institucijos [...] **išsiaiškina**, kad dėl esminio arba svarbaus subjekto padaryto **šios direktyvos 18 ir 20 straipsniuose** nustatytų pareigų pažeidimo [...] **gali būti** pažeistas asmens duomenų saugumas, kaip apibrėžta Reglamento (ES) 2016/679 4 straipsnio 12 dalyje, apie kurį pranešama pagal to reglamento 33 straipsnį, jos, [...] **nepagrįstai nedelsdamos**, informuoja priežiūros institucijas, kompetentingas pagal to reglamento 55 ir 56 straipsnius.
2. Jeigu priežiūros institucijos, kompetentingos pagal Reglamento (ES) 2016/679 55 ir 56 straipsnius, nusprendžia naudotis savo įgaliojimais pagal to reglamento 58 straipsnio **2 dalies** i punktą ir skirti administracinę baudą, **šios direktyvos 8 straipsnyje nurodytos** kompetentingos institucijos neskiria administracinės baudos už [...] **tuo pačiu veiksmu** padarytą pažeidimą [...] pagal šios direktyvos 31 straipsnį. Tačiau kompetentingos institucijos gali taikyti šios direktyvos 29 straipsnio 4 dalies a–i punktuose, 29 straipsnio 5 dalyje ir 30 straipsnio 4 dalies a–h punktuose numatytus vykdymo užtikrinimo veiksmus arba naudotis sankcijų taikymo įgaliojimais.

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

33 straipsnis

Sankcijos

1. Valstybės narės nustato sankcijų, taikomų pažeidus pagal šią direktyvą priimtas nacionalines nuostatas, taisykles ir imasi visų būtinų priemonių užtikrinti, kad šios sankcijos būtų įgyvendinamos. Numatytos sankcijos turi būti veiksmingos, proporcingos ir atgrasomos.
2. Valstybės narės ne vėliau kaip per [dvejus] metus nuo šios direktyvos įsigaliojimo praneša Komisijai apie tas taisykles ir priemones ir nepagrįstai nedelsdamos informuoja ją apie visus vėlesnius joms įtakos turinčius pakeitimus.

34 straipsnis

Savitarpio pagalba

1. Kai esminis arba svarbus subjektas teikia paslaugas daugiau nei vienoje valstybėje narėje arba [...] **teikia paslaugas vienoje ar keliose** valstybėse narėse, tačiau jo tinklų ir informacinės sistemos yra vienoje ar keliose kitose valstybėse narėse, [...] **atitinkamų** valstybių narių [...] kompetentingos institucijos [...] bendradarbiauja ir padeda viena kitai. Tas bendradarbiavimas apima bent tai, kad:

- a) valstybės narės kompetentingos institucijos, taikančios priežiūros arba vykdymo užtikrinimo priemones, per bendrąjį informacinį centrą informuoja kitų atitinkamų valstybių narių kompetentingas institucijas ir su jomis konsultuojasi dėl priežiūros ir vykdymo užtikrinimo priemonių [...];
 - b) kompetentinga institucija gali prašyti kitos kompetentingos institucijos imtis [...] priežiūros arba vykdymo užtikrinimo priemonių;
 - c) kompetentinga institucija, gavusi kitos kompetentingos institucijos pagrįstą prašymą, teikia kitai kompetentingai institucijai pagalbą, **proporcingą jos pačios turimiems ištekliams**, kad [...] priežiūros ar vykdymo užtikrinimo veiksmai galėtų būti įgyvendinami veiksmingai, efektyviai ir nuosekliai. Tokia savitarpio pagalba gali apimti prašymus pateikti informaciją ir priežiūros priemones, įskaitant prašymus atlikti patikrinimus vietoje arba priežiūrą ne vietoje, arba tikslinius saugumo auditus. Kompetentinga institucija, kuriai pateiktas pagalbos prašymas, negali atmesti to prašymo, išskyrus atvejus, kai pasikeitus informacija su kitomis atitinkamomis institucijomis [...] nustatoma, kad institucija nėra kompetentinga suteikti prašomą pagalbą ar **neturi reikiamų išteklių** arba prašoma pagalba nėra proporcinga kompetentingos institucijos [...] vykdomoms priežiūros užduotims, **arba prašymas yra susijęs su informacija ar veikla, kuri yra nesuderinama su tos valstybės narės nacionaliniu saugumu, visuomenės saugumu arba gynyba.**
2. Kai tinkama ir bendru sutarimu, skirtingų valstybių narių kompetentingos institucijos gali vykdyti [...] bendrus priežiūros veiksmus.

VII SKYRIUS

Pereinamojo laikotarpio ir baigiamosios nuostatos

35 straipsnis

Peržiūra

Komisija periodiškai peržiūri šios direktyvos taikymą ir teikia ataskaitą Europos Parlamentui ir Tarybai. Ataskaitoje visų pirma įvertinama I ir II prieduose nurodytų sektorių, pasektorių, subjektų dydžio ir rūšių svarba ekonomikos ir visuomenės veikimui kibernetinio saugumo atžvilgiu.

Peržiūros [...] tikslu [...] Komisija atsižvelgia į [...] CSIRT tinklo ataskaitas apie patirtį, įgytą [...] operatyviniu lygmeniu. Pirmoji ataskaita pateikiama ne vėliau kaip... [54 mėnesiai po šios direktyvos įsigaliojimo dienos].

36 straipsnis

[...]

[...]

[...]

37 straipsnis

Komiteto procedūra

1. Komisijai padeda komitetas. Tas komitetas – tai komitetas, kaip tai suprantama Reglamente (ES) Nr. 182/2011.
2. Kai daroma nuoroda į šią dalį, taikomas Reglamento (ES) Nr. 182/2011 5 straipsnis.
3. Kai komiteto nuomonei gauti būtina rašytinė procedūra, tokia procedūra laikoma baigta be rezultato, jei per nuomonei pateikti nustatytą laikotarpį taip nusprendžia komiteto pirmininkas arba to prašo komiteto narys.

38 straipsnis

Perkėlimas į nacionalinės teisės aktus

1. **Ne vėliau** kaip [...] **24** mėnesiai nuo šios direktyvos įsigaliojimo dienos] valstybės narės priima ir paskelbia [...] įstatymus ir kitus teisės aktus, būtinus, kad būtų laikomasi šios direktyvos. Apie tai jos nedelsdamos praneša Komisijai. Tas priemonės jos taiko nuo ... [viena diena po pirmoje pastraipoje nurodytos datos].
2. Valstybės narės, priimdamos tas nuostatas, daro jose nuorodą į šią direktyvą arba tokia nuoroda daroma jas oficialiai skelbiant. Nuorodos darymo tvarką nustato valstybės narės.

39 straipsnis

Reglamento (ES) Nr. 910/2014 pakeitimas

Reglamento (ES) Nr. 910/2014 19 straipsnis [...] išbraukiamas **nuo ... [šios direktyvos perkėlimo į nacionalinę teisę galutinis terminas]**.

40 straipsnis

Direktyvos (ES) 2018/1972 pakeitimas

Direktyvos (ES) 2018/1972 40 ir 41 straipsniai [...] išbraukiami **nuo ... [šios direktyvos perkėlimo į nacionalinę teisę galutinis terminas]**.

41 straipsnis

Panaikinimas

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

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

42 straipsnis

Įsigaliojimas

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

43 straipsnis

Adresatai

Ši direktyva skirta valstybėms narėms.

Priimta Briuselyje

Europos Parlamento vardu
Pirmininkas

Tarybos vardu
Pirmininkas

I PRIEDAS

SEKTORIAI, PASEKTORIAI IR SUBJEKTŲ RŪŠYS

Sektorius	Pasektorius	Subjekto rūšis
1. Energetika	a) Elektros energija	— Elektros energijos įmonės, nurodytos Direktyvos (ES) 2019/944 ⁽³⁹⁾ 2 straipsnio 57 punkte, atliekančios tos direktyvos 2 straipsnio 12 punkte nurodytą tiekimo funkciją
		— Skirstymo sistemos operatoriai, nurodyti Direktyvos (ES) 2019/944 2 straipsnio 29 punkte
		— Perdavimo sistemos operatoriai, nurodyti Direktyvos (ES) 2019/944 2 straipsnio 35 punkte
		— Gamintojai, nurodyti Direktyvos (ES) 2019/944 2 straipsnio 38 punkte
		— Paskirtieji elektros energijos rinkos operatoriai, nurodyti Reglamento (ES) 2019/943 ⁽⁴⁰⁾ 2 straipsnio 8 punkte
		— Elektros energijos rinkos dalyviai, nurodyti Reglamento (ES) 2019/943 2 straipsnio 25 punkte, teikiantys telkimo, reguliavimo apkrovos arba energijos kaupimo paslaugas, nurodytas Direktyvos (ES) 2019/944 2 straipsnio 18, 20 ir

³⁹ 2019 m. birželio 5 d. Europos Parlamento ir Tarybos direktyva (ES) 2019/944 dėl elektros energijos vidaus rinkos bendrųjų taisyklių, kuria iš dalies keičiama Direktyva 2012/27/ES (OL L 158, 2019 6 14, p. 125).

⁴⁰ Europos Parlamento ir Tarybos reglamentas (ES) 2019/943 dėl elektros energijos vidaus rinkos (OL L 158, 2019 6 14, p. 54).

		59 punktuose
	b) Centralizuotas šilumos ir vėsumos tiekimas	— Centralizuotas šilumos tiekimas arba centralizuotas vėsumos tiekimas, nurodyti Direktyvos (ES) 2018/2001 dėl skatinimo naudoti atsinaujinančiųjų išteklių energiją ⁽⁴¹⁾ 2 straipsnio 19 punkte
	c) Nafta	— Naftotiekių operatoriai
		— Naftos gamybos, perdirbimo ir apdorojimo įrenginių, laikymo ir perdavimo operatoriai
		— Centrinės naftos atsargų saugyklos, nurodytos Tarybos direktyvos 2009/119/EB ⁽⁴²⁾ 2 straipsnio f punkte
	d) Dujos	— Tiekimo įmonės, nurodytos Direktyvos (ES) 2009/73/EB ⁽⁴³⁾ 2 straipsnio 8 punkte
		— Skirstymo sistemos operatoriai, nurodyti Direktyvos 2009/73/EB 2 straipsnio 6 punkte
		— Perdavimo sistemos operatoriai, nurodyti Direktyvos 2009/73/EB 2 straipsnio 4 punkte
		— Laikymo sistemos operatoriai, nurodyti Direktyvos 2009/73/EB 2

⁴¹ 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/2001 dėl skatinimo naudoti atsinaujinančiųjų išteklių energiją (OL L 328, 2018 12 21, p. 82).

⁴² 2009 m. rugsėjo 14 d. Tarybos direktyva 2009/119/EB, kuria valstybės narės įpareigojamos išlaikyti privalomąsias žalios naftos ir (arba) naftos produktų atsargas (OL L 265, 2009 10 9, p. 9).

⁴³ 2009 m. liepos 13 d. Europos Parlamento ir Tarybos direktyva 2009/73/EB dėl gamtinių dujų vidaus rinkos bendrųjų taisyklių, panaikinti Direktyvą 2003/55/EB (OL L 211, 2009 8 14, p. 94).

		straipsnio 10 punkte
		— SGD sistemos operatoriai, nurodyti Direktyvos 2009/73/EB 2 straipsnio 12 punkte
		— Gamtinių dujų įmonės, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 1 punkte
		— Gamtinių dujų perdirbimo ir apdorojimo įrenginių operatoriai
	e) Vandenilis	Vandenilio gamybos, laikymo ir perdavimo operatoriai
2. Transportas	a) Oro transportas	— Oro vežėjai, nurodyti Reglamento (EB) Nr. 300/2008 ⁽⁴⁴⁾ 3 straipsnio 4 punkte, naudojami komerciniais tikslais
		— Oro uosto valdymo organai, nurodyti Direktyvos 2009/12/EB ⁽⁴⁵⁾ 2 straipsnio 2 punkte, oro uostai, nurodyti tos direktyvos 2 straipsnio 1 punkte, įskaitant Reglamento (ES) Nr. 1315/2013 ⁽⁴⁶⁾ II priedo 2 skirsnyje išvardytus pagrindinius oro uostus, ir subjektai, eksploatuojantys oro uostuose esančius papildomus įrenginius
		— Eismo valdymo operatoriai, teikiantys skrydžių valdymo (ATC)

⁴⁴ 2008 m. kovo 11 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 300/2008 dėl civilinės aviacijos saugumo bendrųjų taisyklių ir panaikinant Reglamentą (EB) Nr. 2320/2002 (OL L 97, 2008 4 9, p. 72).

⁴⁵ 2009 m. kovo 11 d. Europos Parlamento ir Tarybos direktyva 2009/12/EB dėl oro uostų mokesčių (OL L 70, 2009 3 14, p. 11).

⁴⁶ 2013 m. gruodžio 11 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1315/2013 dėl Sąjungos transeuropinio transporto tinklo plėtros gairių, kuriuo panaikinamas Sprendimas Nr. 661/2010/ES (OL L 348, 2013 12 20, p. 1).

		paslaugas, nurodytas Reglamento (EB) Nr. 549/2004 ⁽⁴⁷⁾ 2 straipsnio 1 punkte
	b) Geležinkelių transportas	— Infrastruktūros valdytojai, nurodyti Direktyvos 2012/34/ES ⁽⁴⁸⁾ 3 straipsnio 2 punkte
		— Geležinkelio įmonės, nurodytos Direktyvos 2012/34/ES 3 straipsnio 1 punkte, įskaitant Direktyvos 2012/34/ES 3 straipsnio 12 punkte nurodytus paslaugų įrenginių operatorius
	c) Vandens transportas	— Vidaus vandenų, jūrų ir pakrančių keleivinio ir krovininio vandens transporto bendrovės, nurodytos Reglamento (EB) Nr. 725/2004 ⁽⁴⁹⁾ I priede ir priskiriamos jūrų transporto sektoriui, neįskaitant tų bendrovių eksploatuojamų atskirų laivų
		— Uostų, nurodytų Direktyvos 2005/65/EB ⁽⁵⁰⁾ 3 straipsnio 1 punkte, įskaitant jų uosto įrenginius, nurodytus Reglamento (EB) Nr. 725/2004 2 straipsnio 11 punkte, valdymo įstaigos ir subjektai, eksploatuojantys uostuose esančias įmones ir įrenginius

⁴⁷ 2004 m. kovo 10 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 549/2004, nustatantis bendro Europos dangaus sukūrimo pagrindą (pagrindų reglamentas) (OL L 96, 2004 3 31, p. 1).

⁴⁸ 2012 m. lapkričio 21 d. Europos Parlamento ir Tarybos direktyva 2012/34/ES, kuria sukurama bendra Europos geležinkelių erdvė (OL L 343, 2012 12 14, p. 32).

⁴⁹ 2004 m. kovo 31 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 725/2004 dėl laivų ir uostų įrenginių apsaugos stiprinimo (OL L 129, 2004 4 29, p. 6).

⁵⁰ 2005 m. spalio 26 d. Europos Parlamento ir Tarybos direktyva 2005/65/EB dėl uostų apsaugos stiprinimo (OL L 310, 2005 11 25, p. 28).

		— Laivų eismo tarnybų, nurodytų Direktyvos 2002/59/EB ⁽⁵¹⁾ 3 straipsnio o punkte, operatoriai
	d) Kelių transportas	— Kelių direkcijos, nurodytos Komisijos deleguotojo reglamento (ES) 2015/962 ⁽⁵²⁾ 2 straipsnio 12 punkte, atsakingos už eismo valdymo kontrolę, išskyrus viešuosius subjektus, kuriems eismo valdymo arba intelektinių transporto sistemų operatoriaus veikla yra tik neesminė jų bendrosios veiklos dalis.
		— Intelektinių transporto sistemų, nurodytų Direktyvos 2010/40/ES ⁽⁵³⁾ 4 straipsnio 1 punkte, operatoriai
3. Bankininkystė		— Kredito įstaigos, nurodytos Reglamento (ES) Nr. 575/2013 ⁽⁵⁴⁾ 4 straipsnio 1 punkte, išskyrus nurodytas Direktyvos 2013/36/ES 2 straipsnio 5 dalies 8 punkte, kurioms taikoma išimtis pagal Reglamento XX [DORA] 2 straipsnio 4 dalį]

⁵¹ 2002 m. birželio 27 d. Europos Parlamento ir Tarybos direktyva 2002/59/EB, įdiegianti Bendrijos laivų eismo stebėsenos ir informacijos sistemą ir panaikinanti Tarybos direktyvą 93/75/EEB (OL L 208, 2002 8 5, p. 10).

⁵² 2014 m. gruodžio 18 d. Komisijos deleguotasis reglamentas (ES) 2015/962, kuriuo papildomos Europos Parlamento ir Tarybos direktyvos 2010/40/ES nuostatos, susijusios su visoje Europos Sąjungoje teikiamomis tikralaikės eismo informacijos paslaugomis (OL L 157, 2015 6 23, p. 21).

⁵³ 2010 m. liepos 7 d. Europos Parlamento ir Tarybos direktyva 2010/40/ES dėl kelių transporto ir jo sąsajų su kitų rūšių transportu srities intelektinių transporto sistemų diegimo sistemos (OL L 207, 2010 8 6, p. 1).

⁵⁴ 2013 m. birželio 26 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 575/2013 dėl prudencinių reikalavimų kredito įstaigoms ir investicinėms įmonėms ir kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 648/2012 (OL L 176, 2013 6 27, p. 1).

4. Finansų rinkų infrastruktūros objektai		— Prekybos vietų, nurodytų Direktyvos 2014/65/ES ⁽⁵⁵⁾ 4 straipsnio 24 dalyje, operatoriai
		— Pagrindinės sandorio šalys (PSŠ), nurodytos Reglamento (ES) Nr. 648/2012 ⁽⁵⁶⁾ 2 straipsnio 1 punkte
5. Sveikata		— Sveikatos priežiūros paslaugų teikėjai, nurodyti Direktyvos 2011/24/ES ⁽⁵⁷⁾ 3 straipsnio g punkte
		— ES etaloninės laboratorijos, nurodytos Reglamento XXXX/XXXX dėl didelių tarpvalstybinio pobūdžio grėsmių sveikatai ⁵⁸ 15 straipsnyje
		— Subjektai, vykdančys vaistų, nurodytų Direktyvos 2001/83/EB ⁽⁵⁹⁾ 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 priemonės, kurios laikomos kritinėmis esant ekstremaliajai visuomenės sveikatai situacijai

⁵⁵ 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos direktyva 2014/65/ES dėl finansinių priemonių rinkų, kuria iš dalies keičiamos Direktyva 2011/61/ES ir Direktyva 2002/92/EB (OL L 173, 2014 6 12, p. 349).

⁵⁶ 2012 m. liepos 4 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 648/2012 dėl ne biržos išvestinių finansinių priemonių, pagrindinių sandorio šalių ir sandorių duomenų saugyklų (OL L 201, 2012 7 27, p. 1).

⁵⁷ 2011 m. kovo 9 d. Europos Parlamento ir Tarybos direktyva 2011/24/ES dėl pacientų teisių į tarpvalstybines sveikatos priežiūros paslaugas įgyvendinimo (OL L 88, 2011 4 4, p. 45).

⁵⁸ [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]

⁵⁹ 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).

		(toliau – ypatingos svarbos visuomenės sveikatai priemonių sąrašas), kaip nurodyta Reglamento XXXX ⁶⁰ 20 straipsnyje
6. Geriamasis vanduo		Žmonėms vartoti skirtu vandens, nurodyto Tarybos direktyvos 98/83/EB ⁽⁶¹⁾ 2 straipsnio 1 punkte, tiekėjai ir skirstytojai, išskyrus skirstytojus, kuriems žmonėms vartoti skirtu vandens skirstymas yra tik jų bendrosios kitų prekių ir produktų[...] paskirstymo veiklos neesminė dalis
7. Nuotekos		Miesto, buitines ir pramonines nuotekas, nurodytas Tarybos direktyvos 91/271/EEB ⁽⁶²⁾ 2 straipsnio 1–3 punktuose, renkančios, šalinančios ar valančios įmonės, išskyrus įmones, kurioms miesto, buitinių ir pramoninių nuotekų rinkimas, šalinimas ar valymas yra tik neesminė jų bendrosios veiklos dalis. [...]
8. Skaitmeninė infrastruktūra		— Interneto duomenų srautų mainų taško teikėjai
		— DNS paslaugų teikėjai, išskyrus šakninio pavadinimo serverių operatorius
		— Aukščiausio lygio domenų vardų registrai
		— Debesijos kompiuterijos paslaugų

⁶⁰ [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]

⁶¹ 1998 m. lapkričio 3 d. Tarybos direktyva 98/83/EB dėl žmonėms vartoti skirtu vandens kokybės (OL L 330, 1998 12 5, p. 32).

⁶² 1991 m. gegužės 21 d. Tarybos direktyva 91/271/EEB dėl miesto nuotekų valymo (OL L 135, 1991 5 30, p. 40).

		teikėjai
		— Duomenų centrų paslaugų teikėjai
		— Turinio teikimo tinklo teikėjai
		— Patikimumo užtikrinimo paslaugų teikėjai, nurodyti Reglamento (ES) Nr. 910/2014 ⁽⁶³⁾ 3 straipsnio 19 punkte
		— Viešųjų elektroninių ryšių tinklą, nurodytą Direktyvos (ES) 2018/1972 ⁽⁶⁴⁾ 2 straipsnio 8 punkte, teikėjai arba elektroninių ryšių paslaugų, nurodytą Direktyvos (ES) 2018/1972 2 straipsnio 4 punkte, teikėjai, kai jų paslaugos yra viešai prieinamos
8a. IRT paslaugų valdymas (B2B)		— Valdomų paslaugų teikėjai (MSP) — Valdomų saugumo paslaugų teikėjai (MSSP)

⁶³ 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB (OL L 257, 2014 8 28, p. 73).

⁶⁴ 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas (OL L 321, 2018 12 17, p. 36).

9. Viešojo administravimo subjektai		— Centrinės valdžios viešojo administravimo subjektai, kaip apibrėžta valstybės narės pagal nacionalinę teisę — [...] ⁶⁵[...] — [...]
10. Kosmosas		— Valstybėms narėms arba privačiosioms šalims priklausančios, jų valdomos ir eksploatuojamos antžeminės infrastruktūros operatoriai, kurie remia kosminių paslaugų teikimą, išskyrus Direktyvos (ES) 2018/1972 2 straipsnio 8 punkte nurodytų viešųjų elektroninių ryšių tinklų teikėjus

⁶⁵ [...]

II priedas

SEKTORIAI, PASEKTORIAI IR SUBJEKTŲ RŪŠYS

Sektorius	Pasektorius	Subjekto rūšis
1. Pašto ir kurjerių paslaugos		Pašto paslaugų teikėjai, nurodyti Direktyvos 97/67/EB ⁽⁶⁶⁾ 2 straipsnio 1[...] punkte, įskaitant [...] kurjerių paslaugų teikėjus
2. Atliekų tvarkymas		Atliekas tvarkančios įmonės, kaip nurodyta Direktyvos 2008/98/EB ⁽⁶⁷⁾ 3 straipsnio 9 punkte, išskyrus įmones, kurių atliekų tvarkymas nėra jų pagrindinė ekonominė veikla

⁶⁶ 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 I 21, p. 14) **su pakeitimais, padarytais 2008 m. vasario 20 d. Europos Parlamento ir Tarybos direktyva 2008/6/EB, iš dalies keičiančia Direktyvą 97/67/EB, siekiant visiško Bendrijos pašto paslaugų vidaus rinkos suformavimo (OL L 52, 2008 2 27, p. 3).**

⁶⁷ 2008 m. lapkričio 19 d. Europos Parlamento ir Tarybos direktyva 2008/98/EB dėl atliekų ir panaikinti kai kurias direktyvas (OL L 312, 2008 11 22, p. 3).

3. Cheminių medžiagų gamyba ir platinimas		Chemines medžiagas ir [...] mišinius gaminančios[...] ir platinančios įmonės, nurodytos Reglamento (EB) Nr. 1907/2006 ⁽⁶⁸⁾ 3 straipsnio ([...]) 9 ir 14 punktuose, ir įmonės, vykdančios to reglamento 3 straipsnio 3 dalyje nurodytą gaminių gamybą iš tų cheminių medžiagų ar mišinių.
4. Maisto gamyba, perdirbimas ir platinimas		Maisto verslo įmonės, nurodytos Reglamento (EB) Nr. 178/2002 ⁽⁶⁹⁾ 3 straipsnio 2 punkte, užsiimančios didmeniniu platinimu ir pramonine gamyba ir perdirbimu
5. Gamyba	a) Medicinos priemonių ir <i>in vitro</i> diagnostikos medicinos priemonių gamyba	Medicinos priemonės, nurodytos Reglamento (ES) 2017/745 ⁽⁷⁰⁾ 2 straipsnio 1 punkte, ir <i>in vitro</i> diagnostikos medicinos priemonės, nurodytos Reglamento (ES) 2017/746 ⁽⁷¹⁾ 2 straipsnio 2 punkte, gaminantys subjektai, išskyrus 1 priedo 5 punkte nurodytas medicinos priemonės gaminančius subjektus.

⁶⁸ 2006 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1907/2006 dėl cheminių medžiagų registracijos, įvertinimo, autorizacijos ir apribojimų (REACH), įsteigiantis Europos cheminių medžiagų agentūrą, iš dalies keičiantis Direktyvą 1999/45/EB bei panaikinantį Tarybos reglamentą (EEB) Nr. 793/93, Komisijos reglamentą (EB) Nr. 1488/94, Tarybos direktyvą 76/769/EEB ir Komisijos direktyvas 91/155/EEB, 93/67/EEB, 93/105/EB bei 2000/21/EB (OL L 396, 2006 12 30, p. 1).

⁶⁹ 2002 m. sausio 28 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 178/2002, nustatantis maistui skirtų teisės aktų bendruosius principus ir reikalavimus, įsteigiantis Europos maisto saugos tarnybą ir nustatantis su maisto saugos klausimais susijusias procedūras (OL L 31, 2002 2 1, p. 1).

⁷⁰ 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/745 dėl medicinos priemonių, kuriuo iš dalies keičiama Direktyva 2001/83/EB, Reglamentas (EB) Nr. 178/2002 ir Reglamentas (EB) Nr. 1223/2009, ir kuriuo panaikinamos Tarybos direktyvos 90/385/EEB ir 93/42/EEB (OL L 117, 2017 5 5, p. 1).

⁷¹ 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/746 dėl *in vitro* diagnostikos medicinos priemonių, kuriuo panaikinama Direktyva 98/79/EB ir Komisijos sprendimas 2010/227/ES (OL L 117, 2017 5 5, p. 176)

	b) Kompiuterinių, elektroninių ir optinių gaminių gamyba	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 26 skyriuje
	c) Elektros įrangos gamyba	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 27 skyriuje
	d) Kitų, niekur kitur nepriskirtų, mašinų ir įrangos gamyba	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 28 skyriuje
	e) Motorinių transporto priemonių, priekabų ir puspriekabių gamyba	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 29 skyriuje
	f) Kitos transporto įrangos gamyba	Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 30 skyriuje
6. Skaitmeninių paslaugų teikėjai		— Elektroninių prekyviečių teikėjai
		— Interneto paieškos sistemų teikėjai
		— Socialinių tinklų paslaugų platformos teikėjai
