2022 M. GRUODŽIO 14 D. EUROPOS PARLAMENTO IR TARYBOS DIREKTYVOS (ES) 2022/2555 DĖL PRIEMONIŲ AUKŠTAM BENDRAM KIBERNETINIO SAUGUMO LYGIUI VISOJE SĄJUNGOJE UŽTIKRINTI, KURIA IŠ DALIES KEIČIAMAS REGLAMENTAS (ES) NR. 910/2014 IR DIREKTYVA (ES) 2018/1972 IR PANAIKINAMA DIREKTYVA (ES) 2016/1148 (TIS 2 DIREKTYVA) IR NACIONALINIŲ TEISĖS AKTŲ PROJEKTŲ ATITIKTIES LENTELĖ

2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyvos (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (toliau – TIS 2 direktyva)	1. **Lietuvos Respublikos kibernetinio saugumo įstatymo pakeitimo įstatymo projektas (toliau – KSĮ projektas);** 2. **Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymo Nr. XIII-1120 4 straipsnio pakeitimo įstatymo projektas;** 3. **Lietuvos Respublikos elektroninių ryšių įstatymo Nr. IX-2135 3, 8, 36, 45, 51, 74, 82 ir 98 straipsnių pakeitimo įstatymo projektas;** 4. **Lietuvos Respublikos administracinių nusižengimų kodekso 479, 480 ir 589 straipsnių bei priedo pakeitimo įstatymo projektas (toliau – ANK projektas);** 5. 2021–2030 metų nacionalinis pažangos planas, patvirtintas Lietuvos Respublikos Vyriausybės 2020 m. rugsėjo 9 d. nutarimu Nr. 998 „Dėl 2021–2030 metų nacionalinio pažangos plano patvirtinimo“ (toliau – Nacionalinis pažangos planas); 6. Nacionalinė kibernetinio saugumo plėtros programa, patvirtinta Lietuvos Respublikos Vyriausybės 2023 m. rugsėjo 20 d. nutarimu Nr. 746 „Dėl 2023–2030 metų plėtros programos valdytojos Lietuvos Respublikos krašto apsaugos ministerijos nacionalinės kibernetinio saugumo plėtros programos patvirtinimo“ (toliau – Nacionalinė kibernetinio saugumo plėtros programa); 7. Nacionalinės kibernetinio saugumo plėtros programos pažangos priemonės Nr. 06-007-10-05-07 „Stiprinti kibernetinį atsparumą“ aprašas, patvirtintas Lietuvos Respublikos krašto apsaugos ministro 2024 m. vasario 5 d. įsakymu Nr. V-98 „Dėl 2023–2030 metų plėtros programos valdytojos Lietuvos Respublikos krašto apsaugos ministerijos nacionalinės kibernetinio saugumo plėtros programos pažangos priemonės Nr. 06-007-10-05-07 „Stiprinti kibernetinį atsparumą“ aprašo patvirtinimo“ (toliau – Pažangos priemonė); 8. Lietuvos Respublikos elektroninių ryšių įstatymas (suvestinė redakcija nuo 2024-01-01 iki 2024-04-30); 9. Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos nuostatai, patvirtinti Lietuvos Respublikos krašto apsaugos ministro 2013 m. gruodžio 31 d. įsakymu Nr. V-1200 „Dėl Nacionalinio kibernetinio saugumo centro prie krašto apsaugos ministerijos nuostatų ir struktūros patvirtinimo“ (toliau – NKSC nuostatai);	**Direktyvos (kito ES teisės akto) perkėlimo (įgyvendinimo lygis (visiškas, dalinis)**

	10.Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatymas, (suvestinė redakcija nuo 2024-01-01) (toliau – KVĮ); 11. Lietuvos Respublikos Vyriausybės nutarimas „Dėl Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatymo įgyvendinimo“ (toliau – KVĮ įgyvendinantis teisės aktas); 12. Lietuvos Respublikos viešojo administravimo įstatymas (suvestinė redakcija nuo 2024-01-01). 13. Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas. 14. Lietuvos Respublikos civilinio kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas. Civilinis kodeksas. 15. Lietuvos Respublikos viešojo administravimo įstatymas 16. Lietuvos Respublikos elektroninių ryšių įstatymas 17. Lietuvos Respublikos mokslo ir studijų įstatymas	
1 straipsnis. Dalykas		
1. Šia direktyva nustatomos priemonės, kuriomis siekiama užtikrinti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje, kad būtų pagerintas vidaus rinkos veikimas.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
2. Tuo tikslu šia direktyva nustatomos: a) pareigos, kuriomis iš valstybių narių reikalaujama priimti nacionalines kibernetinio saugumo strategijas ir paskirti arba įsteigti kompetentingas institucijas, kibernetinių krizių valdymo institucijas, bendruosius kibernetinio saugumo kontaktinius punktus (toliau – bendrieji kontaktiniai punktai) ir reagavimo į kompiuterių saugumo incidentus tarnybas (CSIRT); b) kibernetinio saugumo rizikos valdymo priemonės ir pareigos pranešti, taikomos I ar II priede nurodytos rūšies subjektams, taip pat subjektams, identifikuotiems kaip ypatingos svarbos subjektai pagal Direktyvą (ES) 2022/2557; c) dalijimosi kibernetinio saugumo informacija taisyklės ir pareigos ja dalytis; d) valstybių narių pareigos priežiūros ir vykdymo užtikrinimo srityse.	**KSĮ projektas** **1 straipsnis. Įstatymo paskirtis ir taikymas** **1. Šis įstatymas nustato kibernetinio saugumo principus, kibernetinio saugumo politiką formuojančias ir ją įgyvendinančias institucijas, jų funkcijas ir įgaliojimus, kibernetinio saugumo subjektų identifikavimo pagrindus ir šių subjektų pareigas, keitimąsi informacija ir tarpinstitucinį bendradarbiavimą, kibernetinio saugumo subjektų atitikties šio įstatymo reikalavimams patikrinimus ir vykdymo užtikrinimo priemones, nacionalinės kibernetinio saugumo sertifikavimo institucijos įgaliojimus, Saugiojo valstybinio duomenų perdavimo tinklo naudojimo pagrindus.**	Visiškas
2 straipsnis. Taikymo sritis		

1. Ši direktyva taikoma I ar II priede nurodytos rūšies viešiesiems ar privatiesiems subjektams, kurie laikomi vidutinėmis įmonėmis pagal Rekomendacijos 2003/361/EB priedo 2 straipsnį arba kurie viršija to straipsnio 1 dalyje nustatytas viršutines ribas, ir kurie teikia paslaugas arba vykdo veiklą Sąjungoje. Šios direktyvos tikslais tos rekomendacijos priedo 3 straipsnio 4 dalis netaikoma.	**KSĮ projektas** **11 straipsnis. Kibernetinio saugumo subjektai** **<...>** **3. Bendrieji esminių subjektų identifikavimo kriterijai:** **1) subjektas teikia paslaugas ir (ar) vykdo veiklą šio įstatymo 1 priede nurodytuose sektoriuose ir viršija vidutinių įmonių darbuotojų skaičių ir finansinius duomenis apibrėžiančias ribas, nustatytas Smulkiojo ir vidutinio verslo plėtros įstatyme;** **<...>** **4. Bendrieji svarbių subjektų identifikavimo kriterijai:** **1) subjektas teikia paslaugas ir (ar) vykdo veiklą šio įstatymo 2 priede nurodytuose sektoriuose ir viršija mažų įmonių darbuotojų skaičių ir finansinius duomenis apibrėžiančias ribas, nustatytas Smulkiojo ir vidutinio verslo plėtros įstatyme;**	Visiškas
2. Nepaisant subjektų dydžio, ši direktyva taip pat taikoma I ar II priede nurodytos rūšies subjektams, kai: a) paslaugas teikia: i) viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai; ii) patikimumo užtikrinimo paslaugų teikėjai; iii) aukščiausio lygio domenų vardų registrai ir domenų vardų sistemos paslaugų teikėjai; b) subjektas yra vienintelis paslaugos, kuri yra būtina siekiant užtikrinti ypatingos svarbos visuomeninės ar ekonominės veiklos vykdymą, teikėjas valstybėje narėje; c) paslaugos, kurią teikia subjektas, sutrikimas galėtų daryti didelį poveikį viešajam saugumui, visuomenės saugumui arba visuomenės sveikatai; d) paslaugos, kurią teikia subjektas, sutrikimas galėtų kelti didelę sisteminę riziką visų pirma sektoriuose, kuriuose toks sutrikimas galėtų daryti tarpvalstybinį poveikį; e) subjektas yra ypatingos svarbos atsižvelgiant į jo konkrečią svarbą konkrečiam sektoriui ar paslaugos rūšiai arba kitiems tarpusavyje priklausomiems sektoriams valstybėje narėje nacionaliniu ar regioniniu lygmeniu; f) subjektas yra:	**KSĮ projektas** **11 straipsnis. Kibernetinio saugumo subjektai** **1. Kibernetinio saugumo subjekto statusą įgyja ir Kibernetinio saugumo subjektų registre registruojami asmenys, atitinkantys bent vieną iš šio straipsnio 3–5 dalyse nurodytų bendrųjų ar specialiųjų kibernetinio saugumo subjektų identifikavimo kriterijų ir šiuose kriterijuose nurodytoms paslaugoms teikti ar veiklai vykdyti valdantys ir (ar) tvarkantys tinklų ir informacines sistemas. Atsižvelgiant į galimą neigiamą poveikį, kurį kibernetinis incidentas gali padaryti kibernetinio saugumo subjektų valdomoms ir (ar) tvarkomoms tinklų ir informacinėms sistemoms, kibernetinio saugumo subjektai skirstomi į esminius kibernetinio saugumo subjektus (toliau – esminiai subjektai) ir svarbius kibernetinio saugumo subjektus (toliau – svarbūs subjektai).** **2. Kibernetinio saugumo subjektai įgyja pareigas, numatytas kibernetinio saugumo subjektams, tik nuo jų įregistravimo Kibernetinio saugumo subjektų registre.** **3. Bendrieji esminių subjektų identifikavimo kriterijai:** **1) subjektas teikia paslaugas ir (ar) vykdo veiklą šio įstatymo 1 priede nurodytuose sektoriuose ir viršija vidutinių įmonių darbuotojų skaičių ir finansinius duomenis apibrėžiančias ribas, nustatytas Smulkiojo ir vidutinio verslo plėtros įstatyme;** **2) subjektas šio įstatymo 1 priede nurodytame skaitmeninės infrastruktūros sektoriuje teikia kvalifikuotas patikimumo užtikrinimo paslaugas, aukščiausio**	Visiškas

i) centrinės valdžios, kaip valstybė narė apibrėžė pagal nacionalinę teisę viešojo administravimo subjektas, arba ii) regioninio lygmens, kaip valstybė narė apibrėžė pagal nacionalinę teisę, kuris, atlikus rizika grindžiamą vertinimą, teikia paslaugas, kurių sutrikimas galėtų daryti didelį poveikį ypatingos svarbos visuomeninei ar ekonominei veiklai, viešojo administravimo subjektas.	**lygio .lt domeno vardų registravimo paslaugas ar domenų vardų sistemos (toliau – DNS) paslaugas, išskyrus šakninių vardų serverių operatorius;** **3) subjektas šio įstatymo 1 priede nurodytame skaitmeninės infrastruktūros sektoriuje teikia viešuosius elektroninių ryšių tinklus ar viešąsias elektroninių ryšių paslaugas ir yra laikomas vidutine įmone pagal Smulkiojo ir vidutinio verslo plėtros įstatymą;** **4) subjektas Krizių valdymo ir civilinės saugos įstatymo nustatyta tvarka yra pripažintas ypatingos svarbos subjektu;** **5) subjektas šio įstatymo 1 priede nurodytame viešojo administravimo sektoriuje teikia paslaugas ir (ar) vykdo veiklą ir yra laikomas centriniu valstybinio administravimo, regioninio administravimo subjektu ir savivaldybių administravimo subjektu pagal Viešojo administravimo įstatymą;** **6) subjektas Valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka valdo ir (ar) tvarko ypatingos svarbos ir (ar) svarbius valstybės informacinius išteklius;** **7) subjektas yra laikomas nacionaliniam saugumui užtikrinti svarbia įmone arba subjekto valdoma ir (ar) tvarkoma tinklų ir informacinė sistema yra įrašyta į nacionaliniam saugumui užtikrinti svarbių įrenginių ir turto sąrašą.** **4. Bendrieji svarbių subjektų identifikavimo kriterijai:** **1) subjektas teikia paslaugas ir (ar) vykdo veiklą šio įstatymo 2 priede nurodytuose sektoriuose ir viršija mažų įmonių darbuotojų skaičių ir finansinius duomenis apibrėžiančias ribas, nustatytas Smulkiojo ir vidutinio verslo plėtros įstatyme;** **2) subjektas teikia paslaugas ir (ar) vykdo veiklą šio įstatymo 1 priede nurodytuose sektoriuose ir viršija mažų įmonių darbuotojų skaičių ir finansinius duomenis apibrėžiančias ribas, tačiau neviršija vidutinių įmonių darbuotojų skaičių ir finansinius duomenis apibrėžiančių ribų, nustatytų Smulkiojo ir vidutinio verslo plėtros įstatyme;** **3) subjektas teikia nekvalifikuotas patikimumo užtikrinimo paslaugas šio įstatymo 1 priede nurodytame skaitmeninės infrastruktūros sektoriuje ir yra laikomas vidutine, maža ar labai maža įmone pagal Smulkiojo ir vidutinio verslo plėtros įstatymą;** **4) subjektas teikia viešuosius elektroninių ryšių tinklus ar viešąsias elektroninių ryšių paslaugas šio įstatymo 1 priede nurodytame skaitmeninės infrastruktūros sektoriuje ir yra laikomas maža ar labai maža įmone pagal Smulkiojo ir vidutinio verslo plėtros įstatymą;**	
3. Nepriklausomai nuo jų dydžio, ši direktyva taikoma subjektams, identifikuotiems kaip ypatingos svarbos subjektai pagal Direktyvą (ES) 2022/2557.		
4. Nepriklausomai nuo jų dydžio, ši direktyva taikoma subjektams, teikiantiems domenų vardų registravimo paslaugas.		
5. Valstybės narės gali numatyti, kad ši direktyva taikoma: a) viešojo administravimo subjektams vietos lygmeniu; b) švietimo įstaigoms, visų pirma tais atvejais, kai jos vykdo ypatingos svarbos mokslinių tyrimų veiklą.		

	5) subjektas valdo ir (ar) tvarko valstybės informacinius išteklius; **6) subjektas teikia domenų vardų registravimo paslaugas;** **7) subjektas teikia elektroninės informacijos prieglobos paslaugas.** **5. Specialieji kibernetinio saugumo subjektų identifikavimo kriterijai:** **1) subjektas yra vienintelis paslaugos, kuri yra būtina siekiant užtikrinti ypatingos svarbos visuomeninės ar ekonominės veiklos vykdymą Lietuvos Respublikoje, teikėjas;** **2) paslaugos, kurią teikia subjektas, sutrikimas galėtų daryti didelį poveikį viešajam saugumui, visuomenės saugumui arba visuomenės sveikatai;** **3) paslaugos, kurią teikia subjektas, sutrikimas galėtų kelti didelę sisteminę riziką sektoriuose, kuriuose toks sutrikimas galėtų daryti tarpvalstybinį poveikį;** **4) subjektas yra ypatingos svarbos atsižvelgiant į jo konkrečią svarbą konkrečiam sektoriui ar paslaugos rūšiai arba kitiems tarpusavyje priklausomiems sektoriams nacionaliniu ar regioniniu lygmeniu;** **5) subjektas šio įstatymo 1 priede nurodytame viešojo administravimo sektoriuje teikia paslaugas ir (ar) vykdo veiklą, kuriai sutrikus galėtų būti didelis poveikis valstybei, institucijoms ar gyventojams, ir yra laikomas teritoriniu valstybinio administravimo subjektu ar regioniniu administravimo subjektu, ar savivaldybių administravimo subjektu pagal Viešojo administravimo įstatymą;** **6) paslaugos, kurią teikia subjektas, sutrikimas galėtų daryti didelį poveikį esminio subjekto teikiamai paslaugai ir (ar) vykdomai veiklai;** **7) subjektas yra paslaugos, kuri yra būtina gyvybiškai svarbioms valstybės funkcijoms atlikti ir valstybinėms mobilizacinėms užduotims vykdyti, teikėjas;** **8) subjektas šio įstatymo 1 priede nurodytame mokslinių tyrimų sektoriuje vykdo ypatingos svarbos mokslinių tyrimų ir eksperimentinės plėtros veiklą;** **6. Vyriausybė nustato identifikavimo pagal specialiuosius kriterijus metodiką, pagal kurią subjektas priskiriamas esminiams arba svarbiems subjektui. Pagal šio straipsnio 5 dalies 5 punkte nurodytą kriterijų identifikuojami tik esminiai subjektai, o pagal šio straipsnio 5 dalies 8 punkte nurodytą kriterijų identifikuojami tik svarbūs subjektai.** **7. Jeigu subjektas atitinka bent vieną šio straipsnio 4 ar 5 dalyse nurodytą kriterijų, kuriuo identifikuojamas esminis subjektas, laikoma, kad subjektas yra esminis subjektas nepriklausomai nuo jo atitikties svarbaus subjekto kriterijams.**	
6. Šia direktyva nedaromas poveikis valstybių narių atsakomybei užtikrinti nacionalinį saugumą ir jų įgaliojimams apsaugoti kitas	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	

esmines valstybines funkcijas, įskaitant valstybės teritorinio vientisumo užtikrinimą ir viešosios tvarkos palaikymą.		
7. Ši direktyva netaikoma viešojo administravimo subjektams, vykdantiems savo veiklą, nacionalinio saugumo, visuomenės saugumo, gynybos ar teisėsaugos srityse, įskaitant nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas.	*Direktyvos 7 dalies nuostatos skirtos bendroms taisyklėms dėl esminių ir svarbių subjektų identifikavimo. Šios taisyklės atsispindi KSĮ projekto 11 straipsnyje, dėstomame ties Direktyvos 2 ir 3 straipsniais.*	
8. Valstybės narės gali atleisti nuo 21 ir 23 straipsniuose nustatytų pareigų konkrečius subjektus, vykdančius veiklą nacionalinio saugumo, visuomenės saugumo, gynybos ar teisėsaugos srityse, įskaitant nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas, arba kurie teikia paslaugas išimtinai šio straipsnio 7 dalyje nurodytiems viešojo administravimo subjektams, tos veiklos ar paslaugų atžvilgiu. Tokiais atvejais VII skyriuje nurodytos priežiūros ir vykdymo užtikrinimo priemonės netaikomos tai konkrečiai veiklai ar paslaugoms. Kai subjektai vykdo tik šioje dalyje nurodytos rūšies veiklą arba teikia tik šioje dalyje nurodytos rūšies paslaugas, valstybės narės taip pat gali nuspręsti atleisti tuos subjektus nuo 3 ir 27 straipsniuose nustatytų pareigų.	**KSĮ projektas** **1 straipsnis. Įstatymo paskirtis ir taikymas** <...> **2. Šis įstatymas netaikomas žvalgybos institucijoms, išskyrus šio įstatymo VII skyrių.**	Visiškas
9. 7 ir 8 dalys netaikomos, kai subjektas veikia kaip patikimumo užtikrinimo paslaugų teikėjas.	*Direktyvos 7 dalies nuostatos skirtos bendroms taisyklėms dėl esminių ir svarbių subjektų identifikavimo. Šios taisyklės atsispindi KSĮ projekto 11 straipsnyje..*	
10. Ši direktyva netaikoma subjektams, kuriems valstybės narės netaiko Reglamento (ES) 2022/2554 pagal to reglamento 2 straipsnio 4 dalį.	**KSĮ projektas** **1 straipsnis. Įstatymo paskirtis ir taikymas** <...> **3. Šio įstatymo 1 ir 2 prieduose nurodytuose sektoriuose veikiantiems ar teikiantiems paslaugas kibernetinio saugumo subjektams netaikomos šio įstatymo 14 straipsnio ir 18 straipsnio 1 dalies 1 punkto nuostatos, jeigu šiems subjektams atskirai šio įstatymo 1 ir 2 prieduose nurodytiems sektoriams taikomuose Europos Sąjungos teisės aktuose keliami reikalavimai įgyvendinti kibernetinio saugumo rizikos valdymo priemones ar pranešti apie didelius kibernetinius incidentus, kurių poveikis yra bent lygiavertis šio įstatymo 14 straipsnyje ar jo pagrindu priimtuose įgyvendinamuosiuose teisės aktuose, 18**	Visiškas

	straipsnio 1 dalies 1 punkte ir 4 dalyje ir (ar) 18 straipsnio 1 dalies 2 punkte ir 5 dalyje nustatytų reikalavimų poveikiui.	
11. Šioje direktyvoje nustatytos pareigos nereiškia, kad bus teikiama informacija, kurios atskleidimas prieštarautų esminiams valstybių narių nacionalinio saugumo, viešojo saugumo ar gynybos interesams.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
12. Ši direktyva taikoma nedarant poveikio Reglamentui (ES) 2016/679, Direktyvai 2002/58/EB, Europos Parlamento ir Tarybos direktyvoms 2011/93/ES (27) ir 2013/40/ES (28) ir Direktyvai (ES) 2022/2557.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
13. Nedarant poveikio SESV 346 straipsniui, informacija, kuri yra konfidenciali pagal Sąjungos ar nacionalines taisykles, kaip antai taisyklės dėl verslo konfidencialumo, turi būti pagal šią direktyvą keičiamasi su Komisija ir kitomis atitinkamomis institucijomis tik tais atvejais, kai toks keitimasis yra būtinas šios direktyvos taikymui. Keičiamasi tik tokia informacija, kuri atitinka keitimosi tikslą ir yra jam proporcinga. Keičiantis informacija saugomas tos informacijos konfidencialumas ir atitinkamų subjektų saugumo ir komerciniai interesai.	**KSĮ projektas** **22 straipsnis. Informacijos, tvarkomos tarpsinstitucinio bendradarbiavimo metu, apsauga** **1. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos šio įstatymo tikslais gauta informacija, įskaitant asmens duomenis ir konfidencialią informaciją, turi teisę keistis tarpusavyje, su kitų valstybių institucijomis, NATO ir Europos Sąjungos institucijomis ir tarptautinėmis organizacijomis tik tiek, kiek tai yra būtina šių institucijų funkcijoms pagal kompetenciją atlikti, atsižvelgiant į keitimosi informacija tikslą ir proporcingumą.** **2. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos, tvarkydamos šio įstatymo tikslais gautą informaciją, saugo įslaptintą informaciją, asmenų saugumo ir komercinius interesus, taip pat pateiktos informacijos konfidencialumą. Šioje dalyje nurodyta informacija teikiama tik tais atvejais, jeigu teisė gauti šią informaciją yra nustatyta įstatymuose ar jų pagrindu priimtuose kituose įgyvendinamuosiuose norminiuose teisės aktuose.** **3. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos šio įstatymo tikslais tvarkomus asmens duomenis tvarko laikydamosi Asmens duomenų teisinės apsaugos įstatymo, Reglamento (ES) 2016/679 ir Asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymu.**	Visiškas
14. Subjektai, kompetentingos institucijos, bendrieji kontaktiniai punktai ir CSIRT tvarko asmens duomenis tiek, kiek tai būtina šios direktyvos tikslais ir laikydamiesi Reglamento (ES) 2016/679, ir toks tvarkymas visų pirma grindžiamas to reglamento 6 straipsniu. Asmens duomenų tvarkymą pagal šią direktyvą viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai vykdo laikydamiesi Sąjungos duomenų apsaugos teisės ir Sąjungos privatumo teisės, visų pirma Direktyvos 2002/58/EB, nuostatų.		
3 straipsnis. Esminiai ir svarbūs subjektai		
1. Šios direktyvos taikymo tikslais esminiais subjektais laikomi šie subjektai:	**KSĮ projektas** **11 straipsnis. Kibernetinio saugumo subjektai**	Visiškas

a) I priede nurodytos rūšies subjektai, kurie viršija vidutinėms įmonėms nustatytas viršutines ribas, nustatytas Rekomendacijos 2003/361/EB priedo 2 straipsnio 1 dalyje; b) kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai ir aukščiausio lygio domenų vardų registrai, taip pat DNS paslaugų teikėjai, nepriklausomai nuo jų dydžio; c) viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai, kurie laikomi vidutinėmis įmonėmis pagal Rekomendacijos 2003/361/EB priedo 2 straipsnį; d) 2 straipsnio 2 dalies f punkto i papunktyje nurodyti viešojo administravimo subjektai; e) visi kiti I arba II priede nurodytos rūšies subjektai, kuriuos valstybė narė identifikavo kaip esminius subjektus pagal 2 straipsnio 2 dalies b-e punktus; f) subjektai, kurie pagal Direktyvą (ES) 2022/2557 identifikuoti kaip ypatingos svarbos subjektai, nurodyti šios direktyvos 2 straipsnio 3 dalyje; g) jei valstybė narė taip numato, subjektai, kuriuos ta valstybė narė ne vėliau kaip 2023 m. sausio 16 d. identifikavo kaip esminių paslaugų operatorius pagal Direktyvą (ES) 2016/1148 arba nacionalinę teisę.	**1. Kibernetinio saugumo subjekto statusą įgyja ir Kibernetinio saugumo subjektų registre registruojami asmenys, atitinkantys bent vieną iš šio straipsnio 3–5 dalyse nurodytų bendrųjų ar specialiųjų kibernetinio saugumo subjektų identifikavimo kriterijų ir šiuose kriterijuose nurodytoms paslaugoms teikti ar veiklai vykdyti valdantys ir (ar) tvarkantys tinklų ir informacines sistemas. Atsižvelgiant į galimą neigiamą poveikį, kurį kibernetinis incidentas gali padaryti kibernetinio saugumo subjektų valdomoms ir (ar) tvarkomoms tinklų ir informacinėms sistemoms, kibernetinio saugumo subjektai skirstomi į esminius kibernetinio saugumo subjektus (toliau – esminiai subjektai) ir svarbius kibernetinio saugumo subjektus (toliau – svarbūs subjektai).** **2. Kibernetinio saugumo subjektai įgyja pareigas, numatytas kibernetinio saugumo subjektams, tik nuo jų įregistravimo Kibernetinio saugumo subjektų registre.** **3. Bendrieji esminių subjektų identifikavimo kriterijai:** **1) subjektas teikia paslaugas ir (ar) vykdo veiklą šio įstatymo 1 priede nurodytuose sektoriuose ir viršija vidutinių įmonių darbuotojų skaičių ir finansinius duomenis apibrėžiančias ribas, nustatytas Smulkiojo ir vidutinio verslo plėtros įstatyme;** **2) subjektas šio įstatymo 1 priede nurodytame skaitmeninės infrastruktūros sektoriuje teikia kvalifikuotas patikimumo užtikrinimo paslaugas, aukščiausio lygio .lt domeno vardų registravimo paslaugas ar domenų vardų sistemos (toliau – DNS) paslaugas, išskyrus šakninių vardų serverių operatorius;** **3) subjektas šio įstatymo 1 priede nurodytame skaitmeninės infrastruktūros sektoriuje teikia viešuosius elektroninių ryšių tinklus ar viešąsias elektroninių ryšių paslaugas ir yra laikomas vidutine įmone pagal Smulkiojo ir vidutinio verslo plėtros įstatymą;** **4) subjektas Krizių valdymo ir civilinės saugos įstatymo nustatyta tvarka yra pripažintas ypatingos svarbos subjektu;** **5) subjektas šio įstatymo 1 priede nurodytame viešojo administravimo sektoriuje teikia paslaugas ir (ar) vykdo veiklą ir yra laikomas centriniu valstybinio administravimo, regioninio administravimo subjektu ir savivaldybių administravimo subjektu pagal Viešojo administravimo įstatymą;** **6) subjektas Valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka valdo ir (ar) tvarko ypatingos svarbos ir (ar) svarbius valstybės informacinius išteklius;**	
2. Šios direktyvos I arba II priede nurodytos rūšies subjektai, kurie nelaikomi esminiais subjektais pagal šio straipsnio 1 dalį, laikomi svarbiais subjektais. Tai apima subjektus, kuriuos valstybė narė identifikavo kaip esminius subjektus pagal 2 straipsnio 2 dalies b–e punktus.		

	7) subjektas yra laikomas nacionaliniam saugumui užtikrinti svarbia įmone arba subjekto valdoma ir (ar) tvarkoma tinklų ir informacinė sistema yra įrašyta į nacionaliniam saugumui užtikrinti svarbių įrenginių ir turto sąrašą. **4. Bendrieji svarbių subjektų identifikavimo kriterijai:** **1) subjektas teikia paslaugas ir (ar) vykdo veiklą šio įstatymo 2 priede nurodytuose sektoriuose ir viršija mažų įmonių darbuotojų skaičių ir finansinius duomenis apibrėžiančias ribas, nustatytas Smulkiojo ir vidutinio verslo plėtros įstatyme;** **2) subjektas teikia paslaugas ir (ar) vykdo veiklą šio įstatymo 1 priede nurodytuose sektoriuose ir viršija mažų įmonių darbuotojų skaičių ir finansinius duomenis apibrėžiančias ribas, tačiau neviršija vidutinių įmonių darbuotojų skaičių ir finansinius duomenis apibrėžiančių ribų, nustatytų Smulkiojo ir vidutinio verslo plėtros įstatyme;** **3) subjektas teikia nekvalifikuotas patikimumo užtikrinimo paslaugas šio įstatymo 1 priede nurodytame skaitmeninės infrastruktūros sektoriuje ir yra laikomas vidutine, maža ar labai maža įmone pagal Smulkiojo ir vidutinio verslo plėtros įstatymą;** **4) subjektas teikia viešuosius elektroninių ryšių tinklus ar viešąsias elektroninių ryšių paslaugas šio įstatymo 1 priede nurodytame skaitmeninės infrastruktūros sektoriuje ir yra laikomas maža ar labai maža įmone pagal Smulkiojo ir vidutinio verslo plėtros įstatymą;** **5) subjektas valdo ir (ar) tvarko valstybės informacinius išteklius;** **6) subjektas teikia domenų vardų registravimo paslaugas;** **7) subjektas teikia prieglobos paslaugas.** **5. Specialieji kibernetinio saugumo subjektų identifikavimo kriterijai:** **1) subjektas yra vienintelis paslaugos, kuri yra būtina siekiant užtikrinti ypatingos svarbos visuomeninės ar ekonominės veiklos vykdymą Lietuvos Respublikoje, teikėjas;** **2) paslaugos, kurią teikia subjektas, sutrikimas galėtų daryti didelį poveikį viešajam saugumui, visuomenės saugumui arba visuomenės sveikatai;** **3) paslaugos, kurią teikia subjektas, sutrikimas galėtų kelti didelę sisteminę riziką sektoriuose, kuriuose toks sutrikimas galėtų daryti tarpvalstybinį poveikį;** **4) subjektas yra ypatingos svarbos atsižvelgiant į jo konkrečią svarbą konkrečiam sektoriui ar paslaugos rūšiai arba kitiems tarpusavyje priklausomiems sektoriams nacionaliniu ar regioniniu lygmeniu;**	

	5) subjektas šio įstatymo 1 priede nurodytame viešojo administravimo sektoriuje teikia paslaugas ir (ar) vykdo veiklą, kuriai sutrikus galėtų būti didelis poveikis valstybei, institucijoms ar gyventojams, ir yra laikomas teritoriniu valstybinio administravimo subjektu ar regioniniu administravimo subjektu, ar savivaldybių administravimo subjektu pagal Viešojo administravimo įstatymą; **6) paslaugos, kurią teikia subjektas, sutrikimas galėtų daryti didelį poveikį esminio subjekto teikiamai paslaugai ir (ar) vykdomai veiklai;** **7) subjektas yra paslaugos, kuri yra būtina gyvybiškai svarbioms valstybės funkcijoms atlikti ir valstybinėms mobilizacinėms užduotims vykdyti, teikėjas;** **8) subjektas šio įstatymo 1 priede nurodytame mokslinių tyrimų sektoriuje vykdo ypatingos svarbos mokslinių tyrimų ir eksperimentinės plėtros veiklą;** **6. Vyriausybė nustato specialiųjų kibernetinio saugumo subjektų identifikavimo kriterijų vertinamuosius dydžius, pagal kuriuos nustatoma asmenų atitiktis specialiesiems kibernetinio saugumo subjektų identifikavimo kriterijams ir, priklausomai nuo konkretaus specialiojo kibernetinio saugumo subjektų identifikavimo kriterijaus vertinamojo dydžio, subjektas priskiriamas esminiams arba svarbiam subjektui. Pagal šio straipsnio 5 dalies 5 punkte nurodytą kriterijų identifikuojami tik esminiai subjektai, o pagal šio straipsnio 5 dalies 8 punkte nurodytą kriterijų identifikuojami tik svarbūs subjektai.** **7. Jeigu subjektas atitinka bent vieną šio straipsnio 4 ar 5 dalyse nurodytą kriterijų, kuriuo identifikuojamas esminis subjektas, laikoma, kad subjektas yra esminis subjektas nepriklausomai nuo jo atitikties svarbaus subjekto kriterijams.**	
3. Ne vėliau kaip 2025 m. balandžio 17 d. valstybės narės sudaro esminių ir svarbių subjektų bei domeno vardo registravimo paslaugas teikiančių subjektų sąrašą. Po tos datos valstybės narės reguliariai ir ne rečiau kaip kas dvejus metus peržiūri tą sąrašą ir, kai tinkama, jį atnaujina. 4. Siekdamos sudaryti 3 dalyje nurodytą sąrašą, valstybės narės reikalauja, kad toje dalyje nurodyti subjektai kompetentingoms institucijoms pateiktų bent šią informaciją: a) subjekto pavadinimą; b) adresą ir naujausius kontaktinius duomenis, įskaitant subjektų el. pašto adresus, IP adresų ruožus ir telefonų numerius; c) kai taikytina, I arba II priede nurodytą atitinkamą sektorių ir subsektorių ir	**KSĮ projektas** **13 straipsnis. Kibernetinio saugumo subjektų registras** **1. Kibernetinio saugumo subjektų registro objektas yra kibernetinio saugumo subjektai.** **2. Kibernetinio saugumo subjektų registro objektas ir jį apibūdinantys duomenys tvarkomi Kibernetinio saugumo informaciniame tinkle.** **4. Kibernetinio saugumo subjektų registrą sudaro šie pagrindiniai duomenys apie kibernetinio saugumo subjektus:** **1) jeigu kibernetinio saugumo subjektas yra juridinis asmuo – kibernetinio saugumo subjekto pavadinimas, juridinio asmens kodas, teisinis statusas, ekonominės veiklos forma, pagrindinės buveinės adresas (jeigu kibernetinio saugumo subjektas nėra įsisteigęs Europos Sąjungoje – pagal šio įstatymo 12 straipsnio 3 dalį paskirto atstovo pavadinimas, teisinis statusas, ekonominės veiklos forma, registracijos numeris, kontaktiniai duomenys (elektroninio pašto**	Visiškas

d) kai taikytina, valstybių narių, kuriose jos teikia į šios direktyvos taikymo sritį patenkančias paslaugas, sąrašą. 3 dalyje nurodyti subjektai nedelsdami ir bet kuriuo atveju ne vėliau kaip per dvi savaites nuo pakeitimo dienos praneša apie bet kokius pagal šios dalies pirmą pastraipą pateiktų duomenų pakeitimus. Komisija, padedant Europos Sąjungos kibernetinio saugumo agentūrai (toliau – ENISA), nepagrįstai nedelsdama pateikia gaires ir šablonus, susijusius su šioje dalyje nustatytomis pareigomis. Valstybės narės gali nustatyti nacionalinius mechanizmus, pagal kuriuos subjektai galėtų užsiregistruoti patys.	**adresas, ryšio numeris) ir adresas) ir kitų juridinių padalinių Europos Sąjungoje adresai, jei kibernetinio saugumo subjektas yra DNS paslaugų teikėjas, aukščiausio lygio domenų vardų registro paslaugas teikiantis subjektas, debesijos kompiuterijos paslaugų teikėjas, duomenų centrų paslaugų teikėjas, turinio teikimo tinklo paslaugų teikėjas, valdomų paslaugų teikėjas, valdomų saugumo paslaugų teikėjas, internetines prekyvietes, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų paslaugų teikėjas (toliau – specialusis subjektas) ar yra domenų vardų registravimo paslaugas teikiantis subjektas;** **2) jeigu kibernetinio saugumo subjektas yra fizinis asmuo – kibernetinio saugumo subjekto vardas, pavardė, asmens kodas, veiklos vykdymo adresas;** **3) kibernetinio saugumo subjekto kontaktiniai duomenys (elektroninio pašto adresas, ryšio numeris);** **4) kibernetinio saugumo subjekto teikiamos paslaugos ir (ar) vykdomos veiklos, atitinkančios šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus;** **5) kibernetinio saugumo subjekto naudojami interneto protokolo (IP) adresų rėžiai;** **6) valstybės, kuriose kibernetinio saugumo subjektas teikia paslaugas ir (ar) vykdo veiklą, nurodytą šio įstatymo 1 ir 2 prieduose nurodytuose sektoriuose ir subsektoriuose;** **7) kibernetinio saugumo subjekto paslaugų teikimui ar veiklai reikšmingos tinklų ir informacinės sistemos;** **8) šio įstatymo 1 ir 2 prieduose nurodytas sektorius, kuriame kibernetinio saugumo subjektas veikia ar teikia paslaugas, subsektorius, subjekto rūšis kibernetinio saugumo subjekto sektorius, subsektorius, subjekto rūšis.** **4. Subjektas, atitinkantis šio įstatymo 11 straipsnio 3-5 dalyse nustatytus kibernetinio saugumo subjektų identifikavimo kriterijus, Kibernetinio saugumo subjektų registro duomenų tvarkytojui pateikia duomenis, nurodytus Kibernetinio saugumo informacinio tinklo nuostatuose, tvirtinamuose Krašto apsaugos ministerijos. Duomenys teikiami šiuose nuostatuose nustatyta tvarka.** **5. Kibernetinio saugumo subjektus registruoja ir išregistruoja Kibernetinio saugumo informacinio tinklo duomenų tvarkytojas Kibernetinio saugumo informacinio tinklo nuostatuose nustatyta tvarka.** **6. Šio įstatymo 1 ir 2 prieduose nurodytos institucijos, atsakingos už kibernetinio saugumo subjektų identifikavimą, dalyvauja kibernetinio saugumo subjektų registravimo procese Kibernetinio saugumo informacinio tinklo nuostatuose nustatyta tvarka.**	

	7. Kibernetinio saugumo subjektų registro duomenų tvarkytojas Kibernetinio saugumo informacinio tinklo nuostatuose nustatytais atvejais ir tvarka identifikuodamas ir registruodamas kibernetinio saugumo subjektus turi teisę neatlygintinai gauti iš identifikuojamų asmenų, kitų valstybės institucijų, valstybės įstaigų, valstybės valdomų įmonių, viešųjų įstaigų, savivaldybių valdomų įmonių ir savivaldybių įstaigų šio straipsnio 5 dalyje nurodytus duomenis ir kitą šiuos duomenis apibūdinančią informaciją, reikalingą kibernetinio saugumo subjektams registruoti. **8. Asmenys turi teisę skųsti sprendimą juos registruoti Kibernetinio saugumo subjektų registre Lietuvos Respublikos administracinių bylų teisenos įstatymo nustatyta tvarka.** **9. Jei kibernetinio saugumo subjektas neatitinka šio įstatymo 11 straipsnio 3–5 dalyse nurodytų kriterijų, jis išregistruojamas iš Kibernetinio saugumo subjektų registro. Kibernetinio saugumo subjektas išregistruojamas iš Kibernetinio saugumo subjektų registro per 20 darbo dienų nuo momento, kai Kibernetinio saugumo subjektų registro duomenų tvarkytojas gauna informacijos, kad kibernetinio saugumo subjektas nebeatitinka šio įstatymo 11 straipsnio 3–5 dalyse nurodytų kriterijų. Kibernetinio saugumo subjektas netenka šiame įstatyme nurodytų kibernetinio saugumo subjektams taikomų pareigų nuo jo išregistravimo iš Kibernetinio saugumo subjektų registro.** **10. Kibernetinio saugumo subjektai šio įstatymo 1 ir 2 prieduose nurodytiems sektoriams, subsektoriams ir subjekto rūšiai priskiriami pagal Ekonominės veiklos rūšių klasifikatorių Kibernetinio saugumo informacinio tinklo nuostatuose nustatyta tvarka.**	
5. Ne vėliau kaip 2025 m. balandžio 17 d., o vėliau – kas dvejus metus kompetentingos institucijos praneša: a) Komisijai ir Bendradarbiavimo grupei esminių ir svarbių subjektų, įtrauktų į sąrašą vadovaujantis 3 dalimi pagal kiekvieną iš I arba II priede nurodytų sektorių ir subsektorių, skaičių, ir b) Komisijai – atitinkamą informaciją apie esminių ir svarbių subjektų, identifikuotų pagal 2 straipsnio 2 dalies b–e punktus, skaičių, I arba II priede nurodytą sektorių ir subsektorių, kuriems jie priklauso, jų teikiamų paslaugų rūšį ir nuostatą iš įtvirtintųjų 2 straipsnio 2 dalies b–e punktuose, pagal kurią jie buvo identifikuoti.	Pranešimas Europos Komisijai pagal 3 str. apie subjektų sąrašą įtrauktas į LINESIS priemonių planą	Dalinis

6. Iki 2025 m. balandžio 17 d. ir Komisijai paprašius, valstybės narės gali pranešti Komisijai 5 dalies b punkte nurodytų esminių ir svarbių subjektų pavadinimus.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes KSĮ projekto 7 straipsnio 2 dalies 18 punkte nustatyta, kad Nacionalinis kibernetinio saugumo centras bendradarbiauja su Europos Sąjungos institucijomis.*	
4 straipsnis. Konkretiems sektoriams taikomi Sąjungos teisės aktai		
1. Jei pagal konkretiems sektoriams taikomus Sąjungos teisės aktus reikalaujama, kad esminiai arba svarbūs subjektai priimtų kibernetinio saugumo rizikos valdymo priemones arba praneštų apie didelius incidentus, ir jei tų reikalavimų poveikis yra bent lygiavertis šioje direktyvoje nustatytų pareigų poveikiui, atitinkamos šios direktyvos nuostatos, įskaitant VII skyriuje įtvirtintas nuostatas dėl priežiūros ir vykdymo užtikrinimo, tokiems subjektams netaikomos. Jei konkretiems sektoriams taikomi Sąjungos teisės aktai taikomi ne visiems konkretaus sektoriaus, kuriam taikoma ši direktyva, subjektams, atitinkamos šios direktyvos nuostatos toliau taikomos subjektams, kuriems netaikomi tie konkretiems sektoriams taikomi Sąjungos teisės aktai.	**KSĮ projektas** **1 straipsnis. Įstatymo paskirtis ir taikymas** <...> **3. Šio įstatymo 1 ir 2 prieduose nurodytuose sektoriuose veikiantiems ar teikiantiems paslaugas kibernetinio saugumo subjektams netaikomos šio įstatymo 14 straipsnio ir 18 straipsnio 1 dalies 1 punkto nuostatos, jeigu šiems subjektams atskirai šio įstatymo 1 ir 2 prieduose nurodytiems sektoriams taikomuose Europos Sąjungos teisės aktuose keliami reikalavimai įgyvendinti kibernetinio saugumo rizikos valdymo priemones ar pranešti apie didelius kibernetinius incidentus, kurių poveikis yra bent lygiavertis šio įstatymo 14 straipsnyje ar jo pagrindu priimtuose įgyvendinamuosiuose teisės aktuose, 18 straipsnio 1 dalies 1 punkte ir 4 dalyje ir (ar) 18 straipsnio 1 dalies 2 punkte ir 5 dalyje nustatytų reikalavimų poveikiui.** **4. Šio straipsnio 3 dalyje nurodytų reikalavimų poveikis yra laikomas lygiaverčiu:** **1) šio įstatymo 14 straipsnyje ar jo pagrindu priimtuose įgyvendinamuosiuose teisės aktuose nustatytų reikalavimų poveikiui, jeigu nustatytos kibernetinio saugumo rizikos valdymo priemonės apima priemones, kuriomis siekiama užtikrinti tinklų ir informacinių sistemų saugumą prieinamumo, autentiškumo, vientisumo ir konfidencialumo atžvilgiu, be to, yra grindžiamos visus pavojus apimančiu požiūriu, įskaitant tinklų ir informacinių sistemų fizinį ir aplinkos saugumą;** **2) šio įstatymo 18 straipsnio 1 dalies 1 punkte ir 4 dalyje nustatytų reikalavimų poveikiui, jeigu yra numatyta reagavimo į kibernetinius incidentus tarnybos neatidėliotina prieiga, kai tinkama, automatinė ir tiesioginė, prie pateiktų pranešimų apie incidentus, o nustatyti reikalavimai pranešti apie didelius incidentus pagal poveikį yra bent lygiaverčiai šio įstatymo 18 straipsnio 1 dalies 1 punkte ir 4 dalyje nustatytiems reikalavimams;** **3) šio įstatymo 18 straipsnio 1 dalies 2 punkte ir 5 dalyje nustatytų reikalavimų poveikiui, jeigu yra numatyta reagavimo į kibernetinius incidentus**	Visiškas
2. Šio straipsnio 1 dalyje nurodytų reikalavimų poveikis laikomas lygiaverčiu šioje direktyvoje nustatytų pareigų poveikiui, jeigu: a) kibernetinio saugumo rizikos valdymo priemonių poveikis yra bent lygiavertis priemonių, nustatytų 21 straipsnio 1 ir 2 dalyse, poveikiui; arba b) konkrečiam sektoriui taikomame Sąjungos teisės akte numatyta CSIRT, kompetentingų institucijų arba bendrųjų kontaktinių punktų pagal šią direktyvą neatidėliotina prieiga, kai tinkama, automatinė ir tiesioginė, prie pateiktų pranešimų apie incidentus ir jei reikalavimai pranešti apie didelius incidentus yra pagal poveikį bent lygiaverčiai šios direktyvos 23 straipsnio 1–6 dalyse nustatytiems reikalavimams.		

	tarnybos neatidėliotina prieiga, kai tinkama, automatinė ir tiesioginė, prie pateiktų pranešimų apie incidentus, o nustatyti reikalavimai pranešti apie didelius incidentus pagal poveikį yra bent lygiaverčiai šio įstatymo 18 straipsnio 1 dalies 2 punkte ir 5 dalyje nustatytiems reikalavimams. **5. Lietuvos Respublikos Vyriausybė šio įstatymo 1 ir 2 prieduose nurodytuose atskiruose sektoriuose politiką formuojančių ministerijų teikimu patvirtina konkrečių šio įstatymo 1 ir 2 prieduose nurodytiems sektoriams taikomų Europos Sąjungos teisės aktų, atitinkančių šio straipsnio 4 dalyje nurodytus kriterijus, sąrašą. Šiame sąraše nustatomi šio įstatymo 1 ir 2 prieduose nurodytiems sektoriams taikomi Europos Sąjungos teisės aktai, atitinkantys bent vieną šio straipsnio 4 dalyje nurodytą kriterijų.** **6. Šio įstatymo nuostatos suderintos su Europos Sąjungos teisės aktais, nurodytais šio įstatymo 3 priede.**	
3. Komisija ne vėliau kaip 2023 m. liepos 17 d. pateikia gaires, kuriomis paaiškinamas 1 ir 2 dalių taikymas. Komisija reguliariai peržiūri tas gaires. Rengdama tas gaires Komisija atsižvelgia į visas Bendradarbiavimo grupės ir ENISA pastabas.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
5 straipsnis. Minimalus suderinimas Šia direktyva valstybėms narėms netrukdoma priimti arba palikti toliau galioti nuostatų, kuriomis užtikrinamas aukštesnio lygio kibernetinis saugumas, su sąlyga, kad tokios nuostatos yra suderinamos su valstybių narių įsipareigojimais, nustatytais Sąjungos teisėje.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
6 straipsnis. Terminų apibrėžtys		
Šioje direktyvoje vartojamų terminų apibrėžtys: 1) tinklų ir informacinė sistema – tai: a) elektroninių ryšių tinklas, kaip apibrėžta Direktyvos (ES) 2018/1972 2 straipsnio 1 punkte; b) bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba c) skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami a ir b punktuose nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> **20. Tinklų ir informacinė sistema – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami šiomis nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais.**	Visiškas

2) tinklų ir informacinių sistemų saugumas – tinklų ir informacinių sistemų pajėgumas tam tikru patikimumo lygiu išlikti atspariems bet kokiam įvykiui, galinčiam sukelti pavojų saugomų, perduodamų ar tvarkomų duomenų, arba teikiamų ar per tas tinklų ir informacines sistemas gaunamų paslaugų prieinamumui, autentiškumui, vientisumui ar konfidencialumui;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> **22. Tinklų ir informacinių sistemų saugumas – tinklų ir informacinių sistemų pajėgumas tam tikru patikimumo lygiu išlikti atspariems bet kokiam įvykiui, galinčiam sukelti pavojų saugomų, perduodamų ar tvarkomų duomenų, arba teikiamų ar per tas tinklų ir informacines sistemas gaunamų paslaugų prieinamumui, autentiškumui, vientisumui ar konfidencialumui.**	
3) kibernetinis saugumas – kibernetinis saugumas, kaip apibrėžta Reglamento (ES) 2019/881 2 straipsnio 1 punkte;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> **27. Šiame įstatyme vartojamos sąvokos „Europos kibernetinio saugumo sertifikavimo schema“, „Europos kibernetinio saugumo sertifikatas“, „akreditavimas“ ir „atitikties vertinimo įstaiga“, „informacinių ir ryšių technologijų produktas“, „informacinių ir ryšių technologijų paslauga“, „informacinių ir ryšių technologijų procesas“, „kibernetinė grėsmė“, „kibernetinis saugumas“ suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2019/881. Sąvokos „Kibernetinio saugumo kompetencijos bendruomenė“, „Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras“, „Nacionalinių koordinavimo centrų tinklas“ šiame įstatyme suprantamos taip, kaip jos vartojamos Reglamente (ES) 2021/887. Sąvokos „patikimumo užtikrinimo paslauga“, „patikimumo užtikrinimo paslaugų teikėjas“, „kvalifikuota patikimumo užtikrinimo paslauga“, „kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas“ šiame įstatyme suprantamos taip, kaip jos apibrėžtos Reglamente (ES) Nr. 910/2014. Sąvoka „interneto paieškos sistema“ šiame įstatyme suprantama taip, kaip ji apibrėžta Reglamente (ES) 2019/1150. Sąvoka „standartas“, „techninė specifikacija“ šiame įstatyme suprantama taip, kaip ji apibrėžta (ES) Nr. 1025/2012. Sąvoka „duomenys“ suprantama taip, kaip apibrėžta Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.**	
4) nacionalinė kibernetinio saugumo strategija – nuosekli valstybės narės sistema, kurioje nustatyti tos valstybės narės kibernetinio saugumo srities strateginiai tikslai ir prioritetai ir jų įgyvendinimo valdymas;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> **15. Nacionalinė kibernetinio saugumo strategija – nuosekli valstybės narės sistema, kurioje nustatyti tos valstybės narės kibernetinio saugumo srities strateginiai tikslai ir prioritetai ir jų įgyvendinimo valdymas.**	

5) vos neįvykęs incidentas – įvykis, kuriuo galėjo būti sukeltas pavojus saugomų, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumui, autentiškumui, vientisumui arba konfidencialumui, bet kuriam įvykti buvo sėkmingai užkirstas kelias arba kuris neįvyko;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **26. Vos neįvykęs kibernetinis incidentas – įvykis, kuriuo galėjo būti sukeltas pavojus saugomų, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumui, autentiškumui, vientisumui arba konfidencialumui, bet kuriam įvykti buvo sėkmingai užkirstas kelias arba kuris neįvyko.**	
6) incidentas – įvykis, kuriuo sukeliamas pavojus saugomų, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumui, autentiškumui, vientisumui arba konfidencialumui;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **12. Kibernetinis incidentas – įvykis, kuriuo sukeliamas pavojus saugomų, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumui, autentiškumui, vientisumui arba konfidencialumui.**	
7) didelio masto kibernetinio saugumo incidentas – incidentas, į kurio sukeltą sutrikimą viena valstybė narė nepajėgia reaguoti arba kuris daro didelį poveikį ne mažiau kaip dviem valstybėms narėms;	**KSĮ projektas** **18 straipsnis. Pranešimai apie kibernetinius incidentus** **1. Kibernetinio saugumo subjektai privalo pranešti Nacionaliniam kibernetinio saugumo centrui apie:** **1) didelį kibernetinį incidentą, darantį poveikį jų šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus atitinkančiai vykdomai veiklai ir (ar) teikiamoms paslaugoms** **KVĮ** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** 16. **Ypatingas įvykis** – staigus įvykis ar netikėtai susidariusios aplinkybės, sukėlę pavojų visuomenės saugumui ar viešajai tvarkai, gyventojų gyvybei, sveikatai, turtui ar aplinkai, užsienio valstybėje esančių Lietuvos Respublikos piliečių gyvybei ar saugumui, nacionalinę priklausomybę turintiems laivams ar orlaiviams, kai staigus įvykis ar netikėtai susidariusios aplinkybės turi ar gali turėti reikšmingų neigiamų padarinių ir (ar) reikia skubaus valdymo sprendimo nacionaliniu lygmeniu.	
8) incidento valdymas – visi veiksmai ir procedūros, kuriais siekiama užkirsti incidentui kelią, atskleisti, išanalizuoti ir sustabdyti incidentą arba į jį reaguoti ir atstatyti veiklą po incidento;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>**	

	11. Kibernetinio incidento valdymas – visi veiksmai ir procedūros, kuriais siekiama užkirsti kibernetiniam incidentui kelią, atskleisti, išanalizuoti ir sustabdyti kibernetinį incidentą arba į jį reaguoti ir atkurti veiklą po kibernetinio incidento.	
9) rizika – potencialus praradimas arba sutrikimas, kurį sukėlė incidentas, kuri turi būti išreikšta kaip tokio praradimo arba sutrikimo masto ir incidento pasikartojimo derinys;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **13. Kibernetinio saugumo rizika – potencialus praradimas arba sutrikimas, kurį sukėlė kibernetinis incidentas, ir kuri turi būti išreikšta kaip tokio praradimo arba sutrikimo masto ir kibernetinio incidento pasikartojimo derinys.**	
10) kibernetinė grėsmė – kibernetinė grėsmė, kaip apibrėžta Reglamento (ES) 2019/881 2 straipsnio 8 punkte;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **27. Šiame įstatyme vartojamos sąvokos „Europos kibernetinio saugumo sertifikavimo schema“, „Europos kibernetinio saugumo sertifikatas“, „akreditavimas“ ir „atitikties vertinimo įstaiga“, „informacinių ir ryšių technologijų produktas“, „informacinių ir ryšių technologijų paslauga“, „informacinių ir ryšių technologijų procesas“, „kibernetinė grėsmė“, „kibernetinis saugumas“ suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2019/881. Sąvokos „Kibernetinio saugumo kompetencijos bendruomenė“, „Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras“, „Nacionalinių koordinavimo centrų tinklas“ šiame įstatyme suprantamos taip, kaip jos vartojamos Reglamente (ES) 2021/887. Sąvokos „patikimumo užtikrinimo paslauga“, „patikimumo užtikrinimo paslaugų teikėjas“, „kvalifikuota patikimumo užtikrinimo paslauga“, „kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas“ šiame įstatyme suprantamos taip, kaip jos apibrėžtos Reglamente (ES) Nr. 910/2014. Sąvoka „interneto paieškos sistema“ šiame įstatyme suprantama taip, kaip ji apibrėžta Reglamente (ES) 2019/1150. Sąvoka „standartas“, „techninė specifikacija“ šiame įstatyme suprantama taip, kaip ji apibrėžta (ES) Nr. 1025/2012. Sąvoka „duomenys“ suprantama taip, kaip apibrėžta Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.**	
11) didelė kibernetinė grėsmė – kibernetinė grėsmė, dėl kurios techninių charakteristikų galima daryti prielaidą, kad ji gali	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos**	

padaryti didelį neigiamą poveikį subjekto tinklų ir informacinėms sistemoms arba subjekto paslaugų naudotojų tinklų ir informacinėms sistemoms, sukeldama didelę turtinę arba neturtinę žalą;	<...> **3. Didelė kibernetinė grėsmė – kibernetinė grėsmė, dėl kurios techninių charakteristikų galima daryti prielaidą, kad ji gali padaryti didelį neigiamą poveikį subjekto arba subjekto paslaugų naudotojų tinklų ir informacinėms sistemoms, sukeldama didelę turtinę arba neturtinę žalą.**	
12) IRT produktas – IRT produktas, kaip apibrėžta Reglamento (ES) 2019/881 2 straipsnio 12 punkte;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> **27. Šiame įstatyme vartojamos sąvokos „Europos kibernetinio saugumo sertifikavimo schema“, „Europos kibernetinio saugumo sertifikatas“, „akreditavimas“ ir „atitikties vertinimo įstaiga“, „informacinių ir ryšių technologijų produktas“, „informacinių ir ryšių technologijų paslauga“, „informacinių ir ryšių technologijų procesas“, „kibernetinė grėsmė“, „kibernetinis saugumas“ suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2019/881. Sąvokos „Kibernetinio saugumo kompetencijos bendruomenė“, „Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras“, „Nacionalinių koordinavimo centrų tinklas“ šiame įstatyme suprantamos taip, kaip jos vartojamos Reglamente (ES) 2021/887. Sąvokos „patikimumo užtikrinimo paslauga“, „patikimumo užtikrinimo paslaugų teikėjas“, „kvalifikuota patikimumo užtikrinimo paslauga“, „kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas“ šiame įstatyme suprantamos taip, kaip jos apibrėžtos Reglamente (ES) Nr. 910/2014. Sąvoka „interneto paieškos sistema“ šiame įstatyme suprantama taip, kaip ji apibrėžta Reglamente (ES) 2019/1150. Sąvoka „standartas“, „techninė specifikacija“ šiame įstatyme suprantama taip, kaip ji apibrėžta (ES) Nr. 1025/2012. Sąvoka „duomenys“ suprantama taip, kaip apibrėžta Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.**	
13) IRT paslauga – IRT paslauga, kaip apibrėžta Reglamento (ES) 2019/881 2 straipsnio 13 punkte;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> **27. Šiame įstatyme vartojamos sąvokos „Europos kibernetinio saugumo sertifikavimo schema“, „Europos kibernetinio saugumo sertifikatas“, „akreditavimas“ ir „atitikties vertinimo įstaiga“, „informacinių ir ryšių technologijų produktas“, „informacinių ir ryšių technologijų paslauga“, „informacinių ir ryšių technologijų procesas“, „kibernetinė grėsmė“, „kibernetinis saugumas“ suprantamos taip, kaip jos apibrėžtos Reglamente (ES)**	

	2019/881. Sąvokos „Kibernetinio saugumo kompetencijos bendruomenė“, „Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras“, „Nacionalinių koordinavimo centrų tinklas“ šiame įstatyme suprantamos taip, kaip jos vartojamos Reglamente (ES) 2021/887. Sąvokos „patikimumo užtikrinimo paslauga“, „patikimumo užtikrinimo paslaugų teikėjas“, „kvalifikuota patikimumo užtikrinimo paslauga“, „kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas“ šiame įstatyme suprantamos taip, kaip jos apibrėžtos Reglamente (ES) Nr. 910/2014. Sąvoka „interneto paieškos sistema“ šiame įstatyme suprantama taip, kaip ji apibrėžta Reglamente (ES) 2019/1150. Sąvoka „standartas“, „techninė specifikacija“ šiame įstatyme suprantama taip, kaip ji apibrėžta (ES) Nr. 1025/2012. Sąvoka „duomenys“ suprantama taip, kaip apibrėžta Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.	
14) IRT procesas – IRT procesas, kaip apibrėžta Reglamento (ES) 2019/881 2 straipsnio 14 punkte;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **27. Šiame įstatyme vartojamos sąvokos „Europos kibernetinio saugumo sertifikavimo schema“, „Europos kibernetinio saugumo sertifikatas“, „akreditavimas“ ir „atitikties vertinimo įstaiga“, „informacinių ir ryšių technologijų produktas“, „informacinių ir ryšių technologijų paslauga“, „informacinių ir ryšių technologijų procesas“, „kibernetinė grėsmė“, „kibernetinis saugumas“ suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2019/881. Sąvokos „Kibernetinio saugumo kompetencijos bendruomenė“, „Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras“, „Nacionalinių koordinavimo centrų tinklas“ šiame įstatyme suprantamos taip, kaip jos vartojamos Reglamente (ES) 2021/887. Sąvokos „patikimumo užtikrinimo paslauga“, „patikimumo užtikrinimo paslaugų teikėjas“, „kvalifikuota patikimumo užtikrinimo paslauga“, „kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas“ šiame įstatyme suprantamos taip, kaip jos apibrėžtos Reglamente (ES) Nr. 910/2014. Sąvoka „interneto paieškos sistema“ šiame įstatyme suprantama taip, kaip ji apibrėžta Reglamente (ES) 2019/1150. Sąvoka „standartas“, „techninė specifikacija“ šiame įstatyme suprantama taip, kaip ji apibrėžta (ES) Nr. 1025/2012. Sąvoka „duomenys“ suprantama taip, kaip apibrėžta Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.**	

15) pažeidžiamumas – IRT produktų arba IRT paslaugų silpnoji vieta, jautrumas ar trūkumas, kuriais gali būti pasinaudota kibernetinei grėsmei kelti;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **21. Tinklų ir informacinės sistemos spraga – tinklų ir informacinės sistemos trūkumas, įskaitant informacinių ir ryšių technologijų produktų arba informacinių ir ryšių technologijų paslaugų trūkumus, dėl kurio gali įvykti kibernetinis incidentas ar kuriuo gali būti pasinaudota kibernetinei grėsmei kelti.**	
16) standartas – standartas, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) Nr. 1025/2012 (29) 2 straipsnio 1 punkte;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **27. Šiame įstatyme vartojamos sąvokos „Europos kibernetinio saugumo sertifikavimo schema“, „Europos kibernetinio saugumo sertifikatas“, „akreditavimas“ ir „atitikties vertinimo įstaiga“, „informacinių ir ryšių technologijų produktas“, „informacinių ir ryšių technologijų paslauga“, „informacinių ir ryšių technologijų procesas“, „kibernetinė grėsmė“, „kibernetinis saugumas“ suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2019/881. Sąvokos „Kibernetinio saugumo kompetencijos bendruomenė“, „Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras“, „Nacionalinių koordinavimo centrų tinklas“ šiame įstatyme suprantamos taip, kaip jos vartojamos Reglamente (ES) 2021/887. Sąvokos „patikimumo užtikrinimo paslauga“, „patikimumo užtikrinimo paslaugų teikėjas“, „kvalifikuota patikimumo užtikrinimo paslauga“, „kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas“ šiame įstatyme suprantamos taip, kaip jos apibrėžtos Reglamente (ES) Nr. 910/2014. Sąvoka „interneto paieškos sistema“ šiame įstatyme suprantama taip, kaip ji apibrėžta Reglamente (ES) 2019/1150. Sąvoka „standartas“, „techninė specifikacija“ šiame įstatyme suprantama taip, kaip ji apibrėžta (ES) Nr. 1025/2012. Sąvoka „duomenys“ suprantama taip, kaip apibrėžta Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.**	
17) techninė specifikacija – techninė specifikacija, kaip apibrėžta Reglamento (ES) Nr. 1025/2012 2 straipsnio 4 punkte;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **27. Šiame įstatyme vartojamos sąvokos „Europos kibernetinio saugumo sertifikavimo schema“, „Europos kibernetinio saugumo sertifikatas“, „akreditavimas“ ir „atitikties vertinimo įstaiga“, „informacinių ir ryšių technologijų produktas“, „informacinių ir ryšių technologijų paslauga“,**	

	„informacinių ir ryšių technologijų procesas“, „kibernetinė grėsmė“, „kibernetinis saugumas“ suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2019/881. Sąvokos „Kibernetinio saugumo kompetencijos bendruomenė“, „Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras“, „Nacionalinių koordinavimo centrų tinklas“ šiame įstatyme suprantamos taip, kaip jos vartojamos Reglamente (ES) 2021/887. Sąvokos „patikimumo užtikrinimo paslauga“, „patikimumo užtikrinimo paslaugų teikėjas“, „kvalifikuota patikimumo užtikrinimo paslauga“, „kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas“ šiame įstatyme suprantamos taip, kaip jos apibrėžtos Reglamente (ES) Nr. 910/2014. Sąvoka „interneto paieškos sistema“ šiame įstatyme suprantama taip, kaip ji apibrėžta Reglamente (ES) 2019/1150. Sąvoka „standartas“, „techninė specifikacija“ šiame įstatyme suprantama taip, kaip ji apibrėžta (ES) Nr. 1025/2012. Sąvoka „duomenys“ suprantama taip, kaip apibrėžta Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.	
18) interneto duomenų srautų mainų taškas – tinklo įrenginys, kuris sudaro sąlygas sujungti daugiau nei du nepriklausomus tinklus (autonomines sistemas), visų pirma siekiant palengvinti interneto duomenų srautų mainus, kuris sujungia tik autonomines sistemas ir kuris nereikalauja, kad interneto duomenų srautai, perduodami tarp bet kurių naudojamų autonominių sistemų porų, būtų perduodami per bet kurią trečią autonominę sistemą ir nekeičia tokių srautų ar kitokiu būdu jų netrikdo;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **9. Interneto duomenų srautų mainų taškas – tinklo įrenginys, kuris sudaro sąlygas sujungti daugiau nei du nepriklausomus tinklus (autonomines sistemas), visų pirma siekiant palengvinti interneto duomenų srautų mainus, kuris sujungia tik autonomines sistemas ir kuris nereikalauja, kad interneto duomenų srautai, perduodami tarp bet kurių naudojamų autonominių sistemų porų, būtų perduodami per bet kurią trečią autonominę sistemą ir nekeičia tokių srautų ar kitokiu būdu jų netrikdo.**	
19) domenų vardų sistema arba DNS – hierarchiškai paskirstyta vardų sistema, kurioje galima identifikuoti interneto paslaugas ir išteklius ir sudaromos sąlygos galutiniams naudotojams naudotis interneto maršruto parinkimo ir junglumo paslaugomis ir gauti tas paslaugas bei išteklius;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **5. Domenų vardų sistema – hierarchiškai paskirstyta vardų sistema, kurioje galima identifikuoti interneto paslaugas ir išteklius ir kurioje sudaromos sąlygos galutiniams naudotojams naudotis interneto maršruto parinkimo ir junglumo paslaugomis ir gauti tas paslaugas bei išteklius.**	
20) DNS paslaugų teikėjas – subjektas, kuris teikia: a) viešai prieinamas rekursinio domenų vardų keitimo paslaugas galutiniams interneto naudotojams arba	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>**	

b) patikimo domenų vardų keitimo paslaugas trečiųjų šalių reikmėms, išskyrus šakninio pavadinimo serverius;	**6. Domenų vardų sistemos paslaugų teikėjas – subjektas, kuris teikia viešai prieinamas rekursinio domenų vardų keitimo paslaugas galutiniams interneto naudotojams arba patikimo domenų vardų keitimo paslaugas trečiųjų šalių reikmėms, išskyrus šakninių vardų serverius.**	
21) aukščiausio lygio domenų vardų registras – subjektas, kuriam pavestas konkretus aukščiausio lygio domenas ir kuris atsako už aukščiausio lygio domeno administravimą, įskaitant to aukščiausio lygio domeno domenų vardų registraciją ir techninį to aukščiausio lygio domeno veikimą, įskaitant jo vardų serverių veikimą, duomenų bazių techninę priežiūrą ir aukščiausio lygio domenų zonos rinkmenų paskirstymą tarp vardų serverių, neatsižvelgiant į tai, ar bet kurias iš tų operacijų atlieka pats subjektas, ar tai yra užsakomosios paslaugos, tačiau neįtraukiant atvejų, kai registras aukščiausio lygio domenų vardus naudoja tik savo reikmėms;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **1. Aukščiausio lygio domenų vardų registro paslaugas teikiantis subjektas – subjektas, atsakingas už aukščiausio lygio domeno administravimą, apimantį domenų vardų registraciją aukščiausio lygio domene ir techninį to aukščiausio lygio domeno veikimą, įskaitant jo vardų serverių veikimą, duomenų bazių techninę priežiūrą ir aukščiausio lygio domenų zonos rinkmenų paskirstymą tarp vardų serverių, neatsižvelgiant į tai, ar bet kurias iš tų operacijų atlieka pats subjektas, ar tai yra užsakomosios paslaugos, neįskaitant atvejų, kai registras aukščiausio lygio domenų vardus naudoja tik savo reikmėms.**	
22) domenų vardų registravimo paslaugas teikiantis subjektas – registratorius arba registratorių vardu veikiantis agentas, pavyzdžiui, privatumo ar įgaliotojo serverio registravimo paslaugų teikėjas arba perpardavėjas;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **4. Domenų vardų registravimo paslaugas teikiantis subjektas – registratorius arba registratorių vardu veikiantis subjektas, įskaitant privatumo ar įgaliotojo tarpininkavimo registravimo paslaugų teikėją arba perpardavėją.**	
23) skaitmeninė paslauga – paslauga, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2015/1535 (30) 1 straipsnio 1 dalies b punkte;	**Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **10. Informacinės visuomenės paslaugos – paprastai už atlyginimą elektroninėmis priemonėmis ir per atstumą individualiu informacinės visuomenės paslaugos gavėjo prašymu teikiamos paslaugos.**	
24) patikimumo užtikrinimo paslauga – patikimumo užtikrinimo paslauga, kaip apibrėžta Reglamento (ES) Nr. 910/2014 3 straipsnio 16 punkte;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **27. Šiame įstatyme vartojamos sąvokos „Europos kibernetinio saugumo sertifikavimo schema“, „Europos kibernetinio saugumo sertifikatas“, „akreditavimas“ ir „atitikties vertinimo įstaiga“, „informacinių ir ryšių technologijų produktas“, „informacinių ir ryšių technologijų paslauga“, „informacinių ir ryšių technologijų procesas“, „kibernetinė grėsmė“,**	

	„kibernetinis saugumas“ suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2019/881. Sąvokos „Kibernetinio saugumo kompetencijos bendruomenė“, „Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras“, „Nacionalinių koordinavimo centrų tinklas“ šiame įstatyme suprantamos taip, kaip jos vartojamos Reglamente (ES) 2021/887. Sąvokos „patikimumo užtikrinimo paslauga“, „patikimumo užtikrinimo paslaugų teikėjas“, „kvalifikuota patikimumo užtikrinimo paslauga“, „kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas“ šiame įstatyme suprantamos taip, kaip jos apibrėžtos Reglamente (ES) Nr. 910/2014. Sąvoka „interneto paieškos sistema“ šiame įstatyme suprantama taip, kaip ji apibrėžta Reglamente (ES) 2019/1150. Sąvoka „standartas“, „techninė specifikacija“ šiame įstatyme suprantama taip, kaip ji apibrėžta (ES) Nr. 1025/2012. Sąvoka „duomenys“ suprantama taip, kaip apibrėžta Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.	
25) patikimumo užtikrinimo paslaugų teikėjas – patikimumo užtikrinimo paslaugų teikėjas, kaip apibrėžta Reglamento (ES) Nr. 910/2014 3 straipsnio 19 punkte;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **27. Šiame įstatyme vartojamos sąvokos „Europos kibernetinio saugumo sertifikavimo schema“, „Europos kibernetinio saugumo sertifikatas“, „akreditavimas“ ir „atitikties vertinimo įstaiga“, „informacinių ir ryšių technologijų produktas“, „informacinių ir ryšių technologijų paslauga“, „informacinių ir ryšių technologijų procesas“, „kibernetinė grėsmė“, „kibernetinis saugumas“ suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2019/881. Sąvokos „Kibernetinio saugumo kompetencijos bendruomenė“, „Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras“, „Nacionalinių koordinavimo centrų tinklas“ šiame įstatyme suprantamos taip, kaip jos vartojamos Reglamente (ES) 2021/887. Sąvokos „patikimumo užtikrinimo paslauga“, „patikimumo užtikrinimo paslaugų teikėjas“, „kvalifikuota patikimumo užtikrinimo paslauga“, „kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas“ šiame įstatyme suprantamos taip, kaip jos apibrėžtos Reglamente (ES) Nr. 910/2014. Sąvoka „interneto paieškos sistema“ šiame įstatyme suprantama taip, kaip ji apibrėžta Reglamente (ES) 2019/1150. Sąvoka „standartas“, „techninė specifikacija“ šiame įstatyme suprantama taip, kaip ji apibrėžta (ES) Nr. 1025/2012. Sąvoka „duomenys“ suprantama taip, kaip apibrėžta Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.**	

26) kvalifikuota patikimumo užtikrinimo paslauga – kvalifikuota patikimumo užtikrinimo paslauga, kaip apibrėžta Reglamento (ES) Nr. 910/2014 3 straipsnio 17 punkte;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **27. Šiame įstatyme vartojamos sąvokos „Europos kibernetinio saugumo sertifikavimo schema“, „Europos kibernetinio saugumo sertifikatas“, „akreditavimas“ ir „atitikties vertinimo įstaiga“, „informacinių ir ryšių technologijų produktas“, „informacinių ir ryšių technologijų paslauga“, „informacinių ir ryšių technologijų procesas“, „kibernetinė grėsmė“, „kibernetinis saugumas“ suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2019/881. Sąvokos „Kibernetinio saugumo kompetencijos bendruomenė“, „Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras“, „Nacionalinių koordinavimo centrų tinklas“ šiame įstatyme suprantamos taip, kaip jos vartojamos Reglamente (ES) 2021/887. Sąvokos „patikimumo užtikrinimo paslauga“, „patikimumo užtikrinimo paslaugų teikėjas“, „kvalifikuota patikimumo užtikrinimo paslauga“, „kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas“ šiame įstatyme suprantamos taip, kaip jos apibrėžtos Reglamente (ES) Nr. 910/2014. Sąvoka „interneto paieškos sistema“ šiame įstatyme suprantama taip, kaip ji apibrėžta Reglamente (ES) 2019/1150. Sąvoka „standartas“, „techninė specifikacija“ šiame įstatyme suprantama taip, kaip ji apibrėžta (ES) Nr. 1025/2012. Sąvoka „duomenys“ suprantama taip, kaip apibrėžta Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.**	
27) kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas – kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, kaip apibrėžta Reglamento (ES) Nr. 910/2014 3 straipsnio 20 punkte;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **27. Šiame įstatyme vartojamos sąvokos „Europos kibernetinio saugumo sertifikavimo schema“, „Europos kibernetinio saugumo sertifikatas“, „akreditavimas“ ir „atitikties vertinimo įstaiga“, „informacinių ir ryšių technologijų produktas“, „informacinių ir ryšių technologijų paslauga“, „informacinių ir ryšių technologijų procesas“, „kibernetinė grėsmė“, „kibernetinis saugumas“ suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2019/881. Sąvokos „Kibernetinio saugumo kompetencijos bendruomenė“, „Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras“, „Nacionalinių koordinavimo centrų tinklas“ šiame įstatyme suprantamos taip, kaip jos vartojamos Reglamente (ES) 2021/887. Sąvokos „patikimumo užtikrinimo paslauga“, „patikimumo užtikrinimo**	

	paslaugų teikėjas“, „kvalifikuota patikimumo užtikrinimo paslauga“, „kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas“ šiame įstatyme suprantamos taip, kaip jos apibrėžtos Reglamente (ES) Nr. 910/2014. Sąvoka „interneto paieškos sistema“ šiame įstatyme suprantama taip, kaip ji apibrėžta Reglamente (ES) 2019/1150. Sąvoka „standartas“, „techninė specifikacija“ šiame įstatyme suprantama taip, kaip ji apibrėžta (ES) Nr. 1025/2012. Sąvoka „duomenys“ suprantama taip, kaip apibrėžta Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.	
28) elektroninė prekyvietė – elektroninė prekyvietė, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2005/29/EB (31) 2 straipsnio n punkte;	**Lietuvos Respublikos civilinio kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas. Civilinis kodeksas** **6.228[1] straipsnis. Vartojimo sutarties samprata ir kitos sąvokos** 13. Elektroninės prekyvietės paslauga – programine įranga, įskaitant interneto svetainę, jos dalį ar taikomąją programą, grindžiama paslauga, kuri teikiama verslininko paties arba jo vardu ir kuria vartotojams suteikiama galimybė sudaryti nuotolines sutartis su kitais verslininkais ar vartotojais.	
29) interneto paieškos sistema – interneto paieškos sistema, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2019/1150 (32) 2 straipsnio 5 punkte;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **27. Šiame įstatyme vartojamos sąvokos „Europos kibernetinio saugumo sertifikavimo schema“, „Europos kibernetinio saugumo sertifikatas“, „akreditavimas“ ir „atitikties vertinimo įstaiga“, „informacinių ir ryšių technologijų produktas“, „informacinių ir ryšių technologijų paslauga“, „informacinių ir ryšių technologijų procesas“, „kibernetinė grėsmė“, „kibernetinis saugumas“ suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2019/881. Sąvokos „Kibernetinio saugumo kompetencijos bendruomenė“, „Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras“, „Nacionalinių koordinavimo centrų tinklas“ šiame įstatyme suprantamos taip, kaip jos vartojamos Reglamente (ES) 2021/887. Sąvokos „patikimumo užtikrinimo paslauga“, „patikimumo užtikrinimo paslaugų teikėjas“, „kvalifikuota patikimumo užtikrinimo paslauga“, „kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas“ šiame įstatyme suprantamos taip, kaip jos apibrėžtos Reglamente (ES) Nr. 910/2014. Sąvoka „interneto paieškos sistema“ šiame įstatyme suprantama taip, kaip ji apibrėžta Reglamente (ES) 2019/1150. Sąvoka „standartas“, „techninė specifikacija“ šiame įstatyme suprantama taip, kaip ji apibrėžta (ES) Nr. 1025/2012. Sąvoka**	

	„duomenys“ suprantama taip, kaip apibrėžta Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.	
30) debesijos kompiuterijos paslauga – skaitmeninė paslauga, kuri pagal poreikį suteikia administravimo paslaugas ir plataus masto nuotolinę prieigą prie kintamo masto pritaikomos bendrų ir paskirstytų kompiuterijos išteklių bazės, įskaitant atvejus, kai tokie ištekliai yra paskirstyti per kelias vietas;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **2. Debesijos kompiuterijos paslauga – informacinės visuomenės paslauga, kuri pagal poreikį suteikia administravimo paslaugas ir plataus masto nuotolinę prieigą prie kintamo masto pritaikomos bendrų ir paskirstytų kompiuterijos išteklių bazės, įskaitant atvejus, kai tokie ištekliai yra paskirstyti per kelias vietas.**	
31) duomenų centro paslauga – paslauga, kuri apima struktūras arba struktūrų grupes, skirtas IT ir tinklo įrangos centralizuotam pritaikymui, tarpusavio junglumui ir eksploatavimui, teikiant duomenų saugojimo, tvarkymo ir transportavimo paslaugas kartu su visa energijos paskirstymo ir aplinkos kontrolės įranga ir infrastruktūra;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **7. 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 perdavimo paslaugas kartu su visa energijos paskirstymo ir aplinkos kontrolės įranga ir infrastruktūra.**	
32) turinio teikimo tinklas – geografiškai paskirstytų serverių tinklas, kurio paskirtis yra turinio ir paslaugų teikėjų vardu užtikrinti interneto naudotojams didelę skaitmeninio turinio ir paslaugų pasiūlą, prieinamumą arba greitą teikimą;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **23. Turinio teikimo tinklas – geografiškai paskirstytų serverių tinklas, kurio paskirtis yra turinio ir paslaugų teikėjų vardu užtikrinti interneto naudotojams didelę skaitmeninio turinio ir paslaugų pasiūlą, prieinamumą arba greitą teikimą.**	
33) socialinių tinklų paslaugų platforma – platforma, kurioje galutiniams naudotojams sudaromos sąlygos prisijungti, dalytis, rasti vienas kitą ir bendrauti naudojant įvairius prietaisus, visų pirma per pokalbius, įrašus, vaizdo įrašus ir rekomendacijas;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **17. Socialinių tinklų paslaugų platforma – interneto platforma, kuri sudaro galimybę galutiniams naudotojams naudojantis įvairiais įrenginiais prisijungti, dalytis turiniu, rasti vienas kitą ir skelbiamą turinį, visų pirma per pokalbius, įrašus, vaizdo įrašus ir rekomendacijas.**	
34) atstovas – Sąjungoje įsisteigęs fizinis arba juridinis asmuo, paskirtas veikti tik DNS paslaugų teikėjo, aukščiausio lygio domenų vardų registro, domenų vardų registravimo paslaugas	**KSĮ projektas** **12 straipsnis. Jurisdikcija ir teritoriškumas** **<...>**	

teikiančio subjekto, debesijos kompiuterijos paslaugų teikėjo, duomenų centro paslaugų teikėjo, turinio pristatymo tinklo paslaugų teikėjo, valdomų paslaugų teikėjo, valdomų saugumo paslaugų teikėjo, elektroninės prekyvietės paslaugų teikėjo, interneto paieškos sistemos paslaugų teikėjo arba socialinio tinklo paslaugų platformų paslaugų teikėjo, kuris nėra įsisteigęs Sąjungoje, vardu, į kurį kompetentinga institucija arba CSIRT gali kreiptis vietoj subjekto dėl to subjekto pareigų pagal šią direktyvą;	**3. Jei šio straipsnio 1 dalies 3 punkte nurodytas subjektas nėra įsisteigęs Europos Sąjungoje, bet teikia paslaugas Lietuvos Respublikoje, jis privalo paskirti Europos Sąjungoje įsisteigusį fizinį arba juridinį asmenį veikti tik DNS paslaugų teikėjo, aukščiausio lygio domenų vardų registro paslaugas teikiančio subjekto, domenų vardų registravimo paslaugas teikiančio subjekto, debesijos kompiuterijos paslaugų teikėjo, duomenų centro paslaugų teikėjo, turinio teikimo tinklo paslaugų teikėjo, valdomų paslaugų teikėjo, valdomų saugumo paslaugų teikėjo, elektroninės prekyvietės paslaugų teikėjo, interneto paieškos sistemos paslaugų teikėjo arba socialinio tinklo paslaugų platformų paslaugų teikėjo, kuris nėra įsisteigęs Europos Sąjungoje, vardu, į kurį Nacionalinis kibernetinio saugumo centras gali kreiptis vietoj subjekto dėl to subjekto pareigų pagal šį įstatymą (toliau – atstovas) Europos Sąjungoje. Šioje dalyje nurodytas atstovas turi būti įsisteigęs vienoje iš tų valstybių narių, kuriose siūlomos paslaugos. Jei šio straipsnio 1 dalies 3 punkte nurodytas subjektas skiria atstovą Lietuvos Respublikoje arba jo nepaskiria, bet teikia paslaugas Lietuvos Respublikoje, laikoma, kad toks subjektas priklauso Lietuvos Respublikos jurisdikcijai.**	
35) viešojo administravimo subjektas – valstybės narės subjektas, kuris valstybėje narėje pagal nacionalinę teisę yra pripažįstamas tokiu subjektu, išskyrus teismines institucijas, parlamentus ir centrinius bankus, ir kuris atitinka šiuos kriterijus: a) yra įsteigtas siekiant tikslo tenkinti bendrojo intereso poreikius, ir nėra pramoninio ar komercinio pobūdžio; b) turi juridinio asmens statusą arba pagal teisės aktus turi teisę veikti kito juridinio asmens statusą turinčio subjekto vardu; c) didžiąja dalimi yra finansuojamas valstybės, regioninių institucijų ar kitų viešosios teisės reglamentuojamų įstaigų lėšomis, arba jam taikoma tų institucijų ar įstaigų administracinė priežiūra, arba jis turi administracinį, valdymo ar priežiūros organą, kurio daugiau kaip pusę narių skiria valstybės, regioninės institucijos arba kitos viešosios teisės reglamentuojamos įstaigos; d) turi įgaliojimus priimti administracinius arba reguliavimo sprendimus dėl fizinių arba juridinių asmenų, kurie daro poveikį jų teisėms tarpvalstybinio asmenų, prekių, paslaugų ar kapitalo judėjimo srityje;	**Lietuvos Respublikos viešojo administravimo įstatymas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** 20. **Viešojo administravimo subjektas** – viešasis juridinis asmuo, valstybės ar savivaldybės valdoma įmonė, kolegiali ar vienasmenė institucija, neturinti juridinio asmens statuso, įstatymų nustatytą specialų statusą turintis fizinis asmuo, šio įstatymo nustatyta tvarka įgalioti atlikti viešąjį administravimą.	

36) viešasis elektroninių ryšių tinklas – viešasis elektroninių ryšių tinklas, kaip apibrėžta Direktyvos (ES) 2018/1972 2 straipsnio 8 punkte;	**Lietuvos Respublikos elektroninių ryšių įstatymas** **3 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** 83. **Viešasis elektroninių ryšių tinklas** – elektroninių ryšių tinklas, kuris visiškai ar daugiausia naudojamas viešosioms elektroninių ryšių paslaugoms teikti ir kuriuo galima perduoti informaciją iš vieno tinklo galinio taško į kitą tinklo galinį tašką.	
37) elektroninių ryšių paslauga – elektroninių ryšių paslauga, kaip apibrėžta Direktyvos (ES) 2018/1972 2 straipsnio 4 punkte;	**Lietuvos Respublikos elektroninių ryšių įstatymas** **3 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** 17. **Elektroninių ryšių paslauga** – elektroninių ryšių tinklais paprastai už atlygį teikiama paslauga: interneto prieigos paslauga, kaip ji apibrėžiama 2015 m. lapkričio 25 d. Europos Parlamento ir Tarybos reglamente (ES) 2015/2120, kuriuo nustatomos priemonės, susijusios su atvira interneto prieiga ir mažmeninėmis reguliuojamų ryšio paslaugų ES viduje kainomis, ir kuriuo iš dalies keičiami Direktyva 2002/22/EB ir Reglamentas (ES) Nr. 531/2012, asmenų tarpusavio ryšio paslauga ir paslauga, kurią visiškai ar daugiausia sudaro signalų perdavimas, kaip antai perdavimo (siuntimo) paslauga, naudojamas įrenginių tarpusavio sąveikos paslaugai teikti ar transliavimui (retransliavimui). Elektroninių ryšių paslauga neapima elektroninių ryšių tinklais ar naudojant elektroninių ryšių paslaugą perduodamos informacijos turinio teikimo ar redakcinės turinio kontrolės paslaugos.	
38) subjektas – fizinis asmuo arba juridinis asmuo, įsteigtas ir tokiu pripažintas pagal jo įsteigimo vietos nacionalinę teisę, kuris, veikdamas savo vardu, naudojasi teisėmis ir kuriam gali būti taikomos pareigos;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **18. Subjektas – fizinis asmuo arba juridinis asmuo, įsteigtas ir tokiu pripažintas pagal jo įsteigimo vietos nacionalinę teisę, kuris, veikdamas savo vardu, naudojasi teisėmis ir kuriam gali būti taikomos pareigos.**	
39) valdomų paslaugų teikėjas – subjektas, teikiantis paslaugas, susijusias su IRT produktų, tinklų, infrastruktūros, taikomųjų programų ar bet kurių kitų tinklų ir informacinių sistemų diegimu, valdymu, naudojimu ar technine priežiūra, teikdamas pagalbą arba aktyvaus administravimo paslaugas klientų patalpose arba nuotoliniu būdu;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** **<...>** **24. Valdomų paslaugų teikėjas – subjektas, teikiantis paslaugas, susijusias su informacinių ir ryšių technologijų produktų, tinklų, infrastruktūros, taikomųjų programų ar bet kurių kitų tinklų ir informacinių sistemų diegimu, valdymu, naudojimu ar technine priežiūra, teikiantis pagalbą arba aktyvaus administravimo paslaugas klientų patalpose arba nuotoliniu būdu.**	

40) valdomų saugumo paslaugų teikėjas – valdomų paslaugų teikėjas, vykdantis veiklą, susijusią su kibernetinio saugumo rizikos valdymu, arba teikiantis pagalbą tokiai veiklai;	**KSĮ projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> **25. Valdomų saugumo paslaugų teikėjas – valdomų paslaugų teikėjas, vykdantis veiklą, susijusią su kibernetinio saugumo rizikos valdymu, arba teikiantis pagalbą tokiai veiklai vykdyti.**	
41) mokslinių tyrimų organizacija – subjektas, kurio pagrindinis tikslas – vykdyti taikomuosius mokslinius tyrimus arba eksperimentinę plėtrą, siekiant panaudoti tų mokslinių tyrimų rezultatus komerciniais tikslais, tačiau kurio veikla neapima švietimo įstaigų.	**Lietuvos Respublikos mokslo ir studijų įstatymas** **4 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> 11. **Lietuvos mokslinių tyrimų institutas** (toliau – mokslinių tyrimų institutas) – Lietuvos Respublikoje įregistruotas juridinis asmuo, kurio pagrindinė veikla – moksliniai tyrimai ir eksperimentinė plėtra.	
7 straipsnis. Nacionalinė kibernetinio saugumo strategija		
1. Kiekviena valstybė narė priima nacionalinę kibernetinio saugumo strategiją, kurioje nustatomi strateginiai tikslai, reikiami ištekliai tiems tikslams pasiekti ir tinkamos politikos bei reguliavimo priemonės, kad būtų pasiektas ir išlaikytas aukšto lygmens kibernetinis saugumas. Nacionalinė kibernetinio saugumo strategija apima: a) valstybės narės kibernetinio saugumo strategijos tikslus ir prioritetus, visų pirma apimančius I ir II prieduose nurodytus sektorius; b) valdymo sistemą, kad būtų pasiekti šios dalies a punkte nurodyti tikslai ir įgyvendinti prioritetai, įskaitant 2 dalyje nurodytą politiką;	**KSĮ projektas** **4 straipsnis. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos** **1. Kibernetinio saugumo politika formuojama, atsižvelgiant į Lietuvos Respublikos Seimo tvirtinamoje Nacionalinio saugumo strategijoje nustatytus ilgojo laikotarpio nacionalinio saugumo politikos prioritetus ir uždavinius, Vyriausybės tvirtinamame Nacionaliniame pažangos plane nustatytus strateginius tikslus ir uždavinius, Seimo tvirtinamoje Krašto apsaugos sistemos stiprinimo ir plėtros bei Vyriausybės tvirtinamose Nacionalinėje kibernetinio saugumo plėtros programose numatytus uždavinių įgyvendinimo prioritetus ir kryptis. Šioje dalyje nurodyti strateginio planavimo dokumentai ar jų dalys, kartu su šiuo įstatymu ir jį įgyvendinančiais teisės aktais sudaro nacionalinę kibernetinio saugumo strategiją.** **Nacionalinis pažangos planas** 1 priedo 10 tikslas „Stiprinti nacionalinį saugumą“ 10.5 uždavinys „Stiprinti kibernetinį saugumą ir gynybą“, už kurį atsakingas strateginio valdymo sistemos dalyvis (dalyvaujantys strateginio valdymo sistemos dalyviai) – KAM ir ministerijos. **Nacionalinė kibernetinio saugumo plėtros programa** Pažangos priemonė, kuria sprendžiama problema:	Dalinis

	06-007-10-05-07 „Stiprinti kibernetinį atsparumą“ (šalinamos 1–4 priežastys). Pažangos priemonės, numatytos kitose plėtros programose: Viešojo saugumo stiprinimo ir plėtros programos pažangos priemonė Nr. 07-011-10-07-01/07-019-10-07-01 „Sudaryti prielaidas veiksmingai nusikaltimų prevencijai ir kontrolei bei terorizmo grėsmių mažinimui“ (šalinama 2 priežastis). *Platesnis Direktyvos 7 straipsnio 1 dalies a ir b punktų įgyvendinimas nėra KSĮ projekto reguliavimo srityje. Numatomas Nacionalinės kibernetinio saugumo plėtros programos tobulinimas.*	
c) valdymo sistemą, pagal kurią paaiškinami atitinkamų suinteresuotųjų subjektų vaidmenys ir pareigos nacionaliniu lygmeniu, kuria grindžiamas kompetentingų institucijų, bendrųjų kontaktinių punktų ir CSIRT pagal šią direktyvą bendradarbiavimas ir veiklos koordinavimas nacionaliniu lygmeniu, taip pat tų įstaigų ir kompetentingų institucijų pagal konkretiems sektoriams taikomus Sąjungos teisės aktus veiklos koordinavimas ir jų bendradarbiavimas;	**KSĮ projektas** **5 straipsnis. Krašto apsaugos ministerijos įgaliojimai kibernetinio saugumo srityje** **Krašto apsaugos ministerija, be šio įstatymo 4 straipsnio 2 dalyje numatyto kibernetinio saugumo politikos formavimo ir kitų šio įstatymo nustatytų funkcijų vykdymo, taip pat bendradarbiauja su atitinkamomis Šiaurės Atlanto sutarties organizacijos (toliau – NATO) bei Europos Sąjungos ir NATO bei Europos Sąjungos valstybių institucijomis, tarptautinėmis institucijomis kibernetinio saugumo klausimais.** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** **1. Nacionalinis kibernetinio saugumo centras yra įstaiga prie Krašto apsaugos ministerijos.** **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** **1) taiko kibernetinių grėsmių paieškos priemones kibernetinėje erdvėje, siekdamas įvertinti tinklų ir informacinių sistemų atsparumą kibernetiniams incidentams;** **2) stebi, renka ir analizuoja informaciją apie kibernetines grėsmes, tinklų ir informacinių sistemų spragas (toliau – spraga), kibernetinius incidentus ir vos neįvykusius kibernetinius incidentus;** **3) valdo kibernetinius incidentus nacionalinio kibernetinių incidentų valdymo plano, tvirtinamo Vyriausybės, nustatyta tvarka;** **4) realiuoju laiku arba beveik realiuoju laiku kibernetinio saugumo subjektams ir suinteresuotiesiems asmenims teikia ankstyvuosius perspėjimus, įspėjimus, pranešimus ir keičiasi informacija apie kibernetines grėsmes, spragas, kibernetinius incidentus ir vos neįvykusius kibernetinius incidentus;**	Visiškas

	5) realiuoju laiku arba beveik realiuoju laiku kibernetinio saugumo subjektams teikia pagalbą, susijusią su jų tinklų ir informacinių sistemų stebėjimu; **6) siekdamas stabdyti kibernetinio incidento poveikį kibernetinio saugumo subjektų tinklų ir informacinių sistemų saugumui, duoda nurodymą viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjams, elektroninių prekyviečių, interneto paieškos sistemų, debesijos kompiuterijos paslaugų teikėjams, elektroninės informacijos prieglobos paslaugų teikėjams ne ilgiau negu 48 valandoms apriboti viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų, elektroninių prekyviečių, interneto paieškos sistemų, debesijos kompiuterijos paslaugų, elektroninės informacijos prieglobos paslaugų teikimą. Nacionalinis kibernetinio saugumo centras apie viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjams pagal šį punktą duotus nurodymus ne vėliau kaip kitą darbo dieną praneša Lietuvos Respublikos ryšių reguliavimo tarnybai;** **7) siekdamas pašalinti kibernetines grėsmes ar stabdyti jų plitimą, duoda nurodymą viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjams, ir (ar) domenų vardų paslaugų teikėjjams blokuoti interneto svetainių, platinančių kenkėjiškus kodus, apgaulės būdu renkančius prisijungimus prie tinklų ir informacinių sistemų ir (ar) naudojamus siekiant koordinuoti ir vykdyti kibernetinius incidentus, domenų vardus, taip pat kitus domenų vardus, sukurtus minėtoms interneto svetainių veikloms vykdyti. Nacionalinio kibernetinio saugumo centro sprendimą blokuoti interneto svetainės domeno vardą jos savininkas turi teisę skųsti teismui Lietuvos Respublikos civilinio proceso kodekso nustatyta tvarka;** **8) kibernetinio incidento metu taiko būtinas kibernetinio saugumo priemones;** **9) tikrina kibernetinio saugumo subjektų valdomas ir (ar) tvarkomas tinklų ir informacines sistemas, siekdamas nustatyti spragas;** **10) koordinuoja spragų atskleidimą;** **11) renka ir analizuoja kibernetinio incidento tyrimo duomenis ir vykdo kibernetinio saugumo rizikų bei kibernetinių incidentų analizę, taip pat užtikrina kibernetinio saugumo politiką formuojančių ir įgyvendinančių institucijų, taip pat kibernetinio saugumo subjektų informavimą apie padėtį kibernetinio saugumo srityje;**	

	12) kai būtina informuoti visuomenę siekiant išvengti kibernetinio incidento arba valdyti vykstantį kibernetinį incidentą arba iškilusią kibernetinę grėsmę, prieš tai pasikonsultavęs su kibernetinio saugumo subjektu, pranešusiu apie kibernetinį incidentą, informuoja visuomenę apie kibernetinį incidentą ir (ar) kibernetinę grėsmę, jeigu įmanoma, nurodydamas veiksmus, kurių būtina imtis reaguojant į tą kibernetinį incidentą ir (ar) kibernetinę grėsmę, arba reikalauja, kad tai padarytų informaciją pateikęs kibernetinio saugumo subjektas; **13) dalyvauja valdant krizes, susijusias su kibernetiniais incidentais, Krizių valdymo ir civilinės saugos įstatymo nustatyta tvarka;** **14) koordinuojant Nacionaliniam krizių valdymo centrui praneša Europos Sąjungos institucijoms apie šio straipsnio 2 dalies 13 punkte nurodytas krizes, kurių viena Lietus Respublika nepajėgia suvaldyti;** **15) dalyvauja Europos Sąjungos ir NATO įsteigtų reagavimo į kibernetinius incidentus tinklų veikloje ir teikia savitarpio pagalbą pagal savo pajėgumus ir kompetenciją kitiems šių tinklų nariams jų prašymu;** **16) atlieka kibernetinio saugumo subjektų atitikties kibernetinio saugumo rizikos valdymo priemonėms stebėseną;** **17) konsultuoja kibernetinio saugumo subjektus kibernetinio saugumo rizikos valdymo priemonių parinkimo ir taikymo klausimais;** **18) bendradarbiauja su Europos Sąjungos, NATO ir kitų valstybių institucijomis ir organizacijomis, įgyvendinančiomis kibernetinio saugumo politiką, tarptautinėmis organizacijomis, turi teisę jas pasitelkti kartu atliekant šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje;** **19) kartu su verslo subjektais, mokslo ir studijų institucijomis, nacionalinėmis, Europos Sąjungos, NATO ir kitų valstybių institucijomis ir organizacijomis, tarptautinėmis organizacijomis, nevyriausybinėmis organizacijomis bei kibernetinio saugumo subjektais plėtoja nacionalinį kibernetinį saugumą stiprinančius projektus;** **20) atlieka kitas šiame įstatyme nustatytas funkcijas.** **3. Nacionalinis kibernetinio saugumo centras, atlikdamas šio straipsnio 2 dalies 16 punkte nurodytas funkcijas, kibernetinio saugumo auditui atlikti turi teisę pasitelkti nepriklausomą auditorių, audito įmonę ar kitą instituciją, kuri atitinka Nacionalinio kibernetinio saugumo centro nustatytas nepriklausomumo, nešališkumo ir nepriekaištingos reputacijos reikalavimus. Kibernetinio saugumo**	

	audito metu turi būti užtikrinamas kibernetinio saugumo subjekto valdomų ir (ar) tvarkomų tinklų ir informacinės sistemos kibernetinis saugumas. **4. Nacionalinio kibernetinio saugumo centro pritaikytas priemones ir nurodymus kibernetinio saugumo subjektai ir kiti asmenys turi teisę skųsti teismui Lietuvos Respublikos administracinių bylų teisenos nustatyta tvarka civilinio proceso kodekso nustatyta tvarka.** **9 straipsnis. Valstybinės duomenų apsaugos inspekcijos įgaliojimai kibernetinio saugumo srityje** **Valstybinė duomenų apsaugos inspekcija įgyvendina kibernetinio saugumo politiką asmens duomenų apsaugos srityje ir atlieka Reglamente (ES) 2016/679 nustatytas priežiūros institucijos užduotis.** **20 straipsnis. Tarpinstitucinis bendradarbiavimas** **1. Kibernetinio saugumo politiką formuojančios ir įgyvendinančios institucijos bendradarbiauja tarpusavyje bei su kitomis valstybės institucijomis įgyvendindamos šiame įstatyme nustatytus tikslus, įskaitant keitimąsi informacija ir duomenimis apie kibernetinius incidentus, kibernetines grėsmes ir vos neįvykusius kibernetinius incidentus, taip pat informacijos perdavimą pagal šio straipsnio 2 dalį.** **2. Nacionalinis kibernetinio saugumo centras:** **1) ne vėliau kaip per 20 darbo dienų nuo sprendimo taikyti šio įstatymo 28 straipsnio 1 dalyje nurodytą vykdymo užtikrinimo priemonę priėmimo apie tai informuoja kompetentingą instituciją pagal Krizių valdymo ir civilinės saugos įstatymą, jeigu vykdymo užtikrinimo priemonė taikoma siekiant užtikrinti, kad esminis subjektas laikytųsi šio įstatymo reikalavimų;** **2) ne vėliau kaip per 20 darbo dienų nuo sprendimo taikyti šio įstatymo 28 straipsnio 1 dalyje vykdymo užtikrinimo priemonę priėmimo apie tai informuoja kompetentingą instituciją pagal Reglamentą (ES) 2022/2554, jeigu vykdymo užtikrinimo priemonė taikoma siekiant užtikrinti, kad esminis subjektas, kuris paskirtas ypatingai svarbiu trečiųjų šalių informacinių ir ryšių technologijų paslaugų teikėju pagal Reglamento (ES) 2022/2554 31 straipsnį, laikytųsi šio įstatymo reikalavimų;** **3) turi teisę su kompetentinga institucija pagal Reglamentą (ES) 2022/2554 sudaryti bendradarbiavimo susitarimą, nurodytą Reglamento (ES) 2022/2554 47 straipsnio 3 dalyje;**	

	4) nustatęs, kad esminis ar svarbus subjektas gali būti padaręs asmens duomenų saugumo pažeidimą, apie tai nepagrįstai nedelsiant, bet ne vėliau kaip per 72 valandas nuo šios aplinkybės nustatymo, informuoja Valstybinę duomenų apsaugos inspekciją nurodydamas turimą informaciją apie Reglamento (ES) 2016/679 33 straipsnio 3 dalyje nurodytas aplinkybes; **5) bendradarbiauja su Lietuvos Respublikos ryšių reguliavimo tarnyba dėl patikimumo užtikrinimo paslaugų teikėjų kibernetinio saugumo audito srityje, ir nedelsiant, be ne vėliau kaip per 24 val. informuoja Lietuvos Respublikos ryšių reguliavimo tarnybą apie patikimumo užtikrinimo paslaugų teikėjų praneštus kibernetinius incidentus;** **6) ne vėliau kaip per 20 darbo dienų nuo sprendimo taikyti šio įstatymo 28 straipsnio 1 dalyje vykdymo užtikrinimo priemonę priėmimo apie tai informuoja kitos valstybės narės kompetentingą instituciją, atsakingą už kibernetinio saugumo reikalavimų vykdymo užtikrinimą, jeigu kibernetinio saugumo subjektas teikia paslaugas arba jo tinklų ir informacinės sistemos yra toje valstybėje narėje;** **7) bendradarbiauja su kitų valstybių narių kompetentingomis institucijos, atsakingomis už kibernetinio saugumo reikalavimų vykdymo užtikrinimą, kai kibernetinio saugumo subjektas teikia paslaugas daugiau nei vienoje valstybėje narėje arba teikia paslaugas vienoje ar daugiau valstybių narių, o jo tinklų ir informacinės sistemos yra vienoje ar daugiau kitų valstybių narių, vykdydamos savitarpio pagalbos prašymus šios įstatymo 21 straipsnio nustatyta tvarka.**	
d) mechanizmą, pagal kurį nustatomi atitinkami objektai, ir kibernetinio saugumo rizikų toje valstybėje narėje vertinimą;	**KSĮ projektas** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** **1) taiko kibernetinių grėsmių paieškos priemones kibernetinėje erdvėje, siekdamas įvertinti tinklų ir informacinių sistemų atsparumą kibernetiniams incidentams;** **2) stebi, renka ir analizuoja informaciją apie kibernetines grėsmes, tinklų ir informacinių sistemų spragas (toliau – spraga), kibernetinius incidentus ir vos neįvykusius kibernetinius incidentus;** <...> **16) atlieka kibernetinio saugumo subjektų atitikties kibernetinio saugumo rizikos valdymo priemonėms stebėseną.**	Visiškas

e) parengties, reagavimo į incidentus ir veiklos po incidento atstatymo priemonių, įskaitant viešojo ir privačiojo sektorių bendradarbiavimą, nustatymą;	**KSĮ projektas** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** **<...>** **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** **1) taiko kibernetinių grėsmių paieškos priemones kibernetinėje erdvėje, siekdamas įvertinti tinklų ir informacinių sistemų atsparumą kibernetiniams incidentams;** **2) stebi, renka ir analizuoja informaciją apie kibernetines grėsmes, tinklų ir informacinių sistemų spragas (toliau – spraga), kibernetinius incidentus ir vos neįvykusius kibernetinius incidentus;** **3) valdo kibernetinius incidentus nacionalinio kibernetinių incidentų valdymo plano, tvirtinamo Vyriausybės, nustatyta tvarka;** **4) realiuoju laiku arba beveik realiuoju laiku kibernetinio saugumo subjektams ir suinteresuotiesiems asmenims teikia ankstyvuosius perspėjimus, įspėjimus, pranešimus ir keičiasi informacija apie kibernetines grėsmes, spragas, kibernetinius incidentus ir vos neįvykusius kibernetinius incidentus;** **5) realiuoju laiku arba beveik realiuoju laiku kibernetinio saugumo subjektams teikia pagalbą, susijusią su jų tinklų ir informacinių sistemų stebėjimu;** **<...>** **8) kibernetinio incidento metu taiko būtinas kibernetinio saugumo priemones;** **<...>** **14) koordinuojant Nacionaliniam krizių valdymo centrui praneša Europos Sąjungos institucijoms apie šio straipsnio 2 dalies 13 punkte nurodytas krizes, kurių viena valstybė narė nepajėgia suvaldyti;** **<...>** **19) kartu su verslo subjektais, mokslo ir studijų institucijomis, nacionalinėmis, Europos Sąjungos, NATO ir kitų valstybių institucijomis ir organizacijomis, tarptautinėmis organizacijomis, nevyriausybinėmis organizacijomis bei kibernetinio saugumo subjektais plėtoja nacionalinį kibernetinį saugumą stiprinančius projektus.** *Platesnis Direktyvos 7 straipsnio 1 dalies e punkto įgyvendinimas nėra KSĮ projekto reguliavimo srityje. Numatomas Nacionalinio incidentų valdymo plano tobulinimas.*	Dalinis

f) įvairių institucijų ir suinteresuotųjų subjektų, dalyvaujančių įgyvendinant nacionalinę kibernetinio saugumo strategiją, sąrašą;	**KSĮ projektas** **4 straipsnis. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos** **1. Kibernetinio saugumo politika formuojama, atsižvelgiant į Lietuvos Respublikos Seimo tvirtinamoje Nacionalinio saugumo strategijoje nustatytus ilgojo laikotarpio nacionalinio saugumo politikos prioritetus ir uždavinius, Vyriausybės tvirtinamame Nacionaliniame pažangos plane nustatytus strateginius tikslus ir uždavinius, Seimo tvirtinamoje Krašto apsaugos sistemos stiprinimo ir plėtros bei Vyriausybės tvirtinamose Nacionalinėje kibernetinio saugumo plėtros programose numatytus uždavinių įgyvendinimo prioritetus ir kryptis. Šioje dalyje nurodyti strateginio planavimo dokumentai sudaro nacionalinę kibernetinio saugumo strategiją.** **Nacionalinis pažangos planas** 1 priedo 10 tikslas „Stiprinti nacionalinį saugumą“; 10.5 uždavinys „Stiprinti kibernetinį saugumą ir gynybą“, už kurį atsakingas strateginio valdymo sistemos dalyvis (dalyvaujantys strateginio valdymo sistemos dalyviai) – KAM ir ministerijos. **Nacionalinė kibernetinio saugumo plėtros programa** Pažangos priemonė, kuria sprendžiama problema: 06-007-10-05-07 „Stiprinti kibernetinį atsparumą“ (šalinamos 1–4 priežastys). Pažangos priemonės, numatytos kitose plėtros programose: Viešojo saugumo stiprinimo ir plėtros programos pažangos priemonė Nr. 07-011-10-07-01/07-019-10-07-01 „Sudaryti prielaidas veiksmingai nusikaltimų prevencijai ir kontrolei bei terorizmo grėsmių mažinimui“ (šalinama 2 priežastis). **Pažangos priemonė** III skyrius, lentelės 3 stulpelis Nacionalinis kibernetinio saugumo centras, Kertinis valstybės telekomunikacijų centras, Policijos departamentas prie Vidaus reikalų ministerijos, Krašto apsaugos ministerija, Nacionalinio koordinavimo centro funkcijas vykdanti institucija, Smulkaus ir vidutinio verslo įmonės.	Dalinis

	Platesnis Direktyvos 7 straipsnio 1 dalies f punkto įgyvendinimas nėra KSĮ projekto reguliavimo srityje. Numatomas Nacionalinės kibernetinio saugumo plėtros programos tobulinimas.	
g) politikos sistemą, padedančią užtikrinti geresnį kompetentingų institucijų pagal šią direktyvą ir kompetentingų institucijų pagal Direktyvą (ES) 2022/2557 koordinavimą siekiant dalytis informacija apie rizikas, kibernetines grėsmes, ir incidentus, taip pat apie nekibernetinę riziką, grėsmes ir incidentus bei, prireikus, vykdyti priežiūros užduotis;	**KSĮ projektas** **20 straipsnis. Tarpinstitucinis bendradarbiavimas** **1. Kibernetinio saugumo politiką formuojančios ir įgyvendinančios institucijos bendradarbiauja tarpusavyje bei su kitomis valstybės institucijomis įgyvendindamos šiame įstatyme nustatytus tikslus, įskaitant keitimąsi informacija ir duomenimis apie kibernetinius incidentus, kibernetines grėsmes ir vos neįvykusius kibernetinius incidentus, taip pat informacijos perdavimą pagal šio straipsnio 2 dalį.** **2. Nacionalinis kibernetinio saugumo centras:** **1) ne vėliau kaip per 20 darbo dienų nuo sprendimo taikyti šio įstatymo 28 straipsnio 1 dalyje nurodytą vykdymo užtikrinimo priemonę priėmimo apie tai informuoja kompetentingą instituciją pagal Krizių valdymo ir civilinės saugos įstatymą, jeigu vykdymo užtikrinimo priemonė taikoma siekiant užtikrinti, kad esminis subjektas laikytųsi šio įstatymo reikalavimų;** **2) ne vėliau kaip per 20 darbo dienų nuo sprendimo taikyti šio įstatymo 28 straipsnio 1 dalyje vykdymo užtikrinimo priemonę priėmimo apie tai informuoja kompetentingą instituciją pagal Reglamentą (ES) 2022/2554, jeigu vykdymo užtikrinimo priemonė taikoma siekiant užtikrinti, kad esminis subjektas, kuris paskirtas ypatingai svarbiu trečiųjų šalių informacinių ir ryšių technologijų paslaugų teikėju pagal Reglamento (ES) 2022/2554 31 straipsnį, laikytųsi šio įstatymo reikalavimų;** **3) turi teisę su kompetentinga institucija pagal Reglamentą (ES) 2022/2554 sudaryti bendradarbiavimo susitarimą, nurodytą Reglamento (ES) 2022/2554 47 straipsnio 3 dalyje;** **4) nustatęs, kad esminis ar svarbus subjektas gali būti padaręs asmens duomenų saugumo pažeidimą, apie tai nepagrįstai nedelsiant, bet ne vėliau kaip per 72 valandas nuo šios aplinkybės nustatymo, informuoja Valstybinę duomenų apsaugos inspekciją nurodydamas turimą informaciją apie Reglamento (ES) 2016/679 33 straipsnio 3 dalyje nurodytas aplinkybes;** **5) bendradarbiauja su Lietuvos Respublikos ryšių reguliavimo tarnyba dėl patikimumo užtikrinimo paslaugų teikėjų kibernetinio saugumo audito srityje, ir nedelsiant, be ne vėliau kaip per 24 val. informuoja Lietuvos**	Visiškas

	Respublikos ryšių reguliavimo tarnybą apie patikimumo užtikrinimo paslaugų teikėjų praneštus kibernetinius incidentus; **6) ne vėliau kaip per 20 darbo dienų nuo sprendimo taikyti šio įstatymo 28 straipsnio 1 dalyje vykdymo užtikrinimo priemonę priėmimo apie tai informuoja kitos valstybės narės kompetentingą instituciją, atsakingą už kibernetinio saugumo reikalavimų vykdymo užtikrinimą, jeigu kibernetinio saugumo subjektas teikia paslaugas arba jo tinklų ir informacinės sistemos yra toje valstybėje narėje;** **7) bendradarbiauja su kitų valstybių narių kompetentingomis institucijos, atsakingomis už kibernetinio saugumo reikalavimų vykdymo užtikrinimą, kai kibernetinio saugumo subjektas teikia paslaugas daugiau nei vienoje valstybėje narėje arba teikia paslaugas vienoje ar daugiau valstybių narių, o jo tinklų ir informacinės sistemos yra vienoje ar daugiau kitų valstybių narių, vykdydamos savitarpio pagalbos prašymus šios įstatymo 21 straipsnio nustatyta tvarka.**	
h) planą, įskaitant būtinas priemones, piliečių informuotumo apie kibernetinį saugumą bendram lygiui didinti.	**Nacionalinis pažangos planas** 1 priedo 10 tikslas „Stiprinti nacionalinį saugumą“ 10.5 uždavinys „Stiprinti kibernetinį saugumą ir gynybą“, už kurį atsakingas strateginio valdymo sistemos dalyvis (dalyvaujantys strateginio valdymo sistemos dalyviai) – KAM ir ministerijos. **Pažangos priemonė** 4. Žinių bei įgūdžių kibernetinio saugumo srityje plėtra 4.1. Kibernetinio saugumo subjektuose dirbančių darbuotojų, kibernetinio saugumo specialistų kompetencijų bei įgūdžių kibernetinio saugumo srityje stiprinimas bei pažeidžiamiausių visuomenės grupių kibernetinio saugumo brandos kėlimas (P-06-007-10-05-07-11 Parengta mokymo medžiaga, reikalinga kibernetinio saugumo kompetencijoms ugdyti (vnt.); P-06-007-10-05-07-03 Užbaigti kibernetinio saugumo mokymai (asm.); P-06-007-10-05-07-12 Kvalifikacijos kėlimo mokymuose dalyvavusių asmenų, dirbančių kibernetinio saugumo srityje, skaičius (asm.); P-06-007-10-05-07-13 Mokymuose dalyvavusių pažeidžiamiausių visuomenės grupių skaičius (vnt.); R-06-007-10-05-07-06 Švietimo ar mokymo veiklos dalyvių skaičius (asm.); R-06-007-10-05-07-07 Švietimo ar mokymo veiklos dalyvių skaičius: iš jų skaitmeninių įgūdžių ugdymo veiklos dalyvių skaičius (asm.) 7. Kibernetinio saugumo valdysenos stiprinimas	Dalinis

	7.1. Kibernetinio saugumo valdysenos Lietuvoje stiprinimas (P-06-007-10-05-07-24 Komunikacijos kampanijų, skirtų visuomenės kibernetinio saugumo brandai didinti, sukūrimo ir sklaidos paslaugų skaičius (vnt.)). *Platesnis Direktyvos 7 straipsnio 1 dalies h punkto įgyvendinimas nėra KSĮ projekto reguliavimo srityje. Numatomas Nacionalinės kibernetinio saugumo plėtros programos tobulinimas.*	
2. Nacionalinėje kibernetinio saugumo strategijoje valstybės narės visų pirma nustato: a) politiką dėl IRT produktų ir IRT paslaugų, kuriuos subjektai naudoja teikdami savo paslaugas, tiekimo grandinių kibernetinio saugumo;	**KSĮ projektas** **14 straipsnis. Kibernetinio saugumo rizikos valdymo priemonės** **1. Kibernetinio saugumo subjektai privalo užtikrinti šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus atitinkančiai veiklai vykdyti ar paslaugoms teikti naudojamų tinklų ir informacinių sistemų atitiktį kibernetinio saugumo rizikos valdymo priemonėms:** **1) kibernetinio saugumo reikalavimams, tvirtinamiems Vyriausybės, išskyrus šio straipsnio 2 dalyje nurodytus atvejus;** **2) Europos Komisijos priimtiems įgyvendinimo aktams, pagal šio straipsnio 3 dalyje nurodytas priemones nustatantiems techninius ir metodinius reikalavimus.** **<...>** **5. Kibernetinio saugumo reikalavimai apima šiuos elementus:** **<...>** **5) tiekimo grandinės saugumą, įskaitant aspektus, susijusius su kiekvieno kibernetinio saugumo subjekto ir jo tiesioginių tiekėjų ar paslaugų teikėjų santykius.** *Platesnis Direktyvos 7 straipsnio 2 dalies a punkto įgyvendinimas nėra KSĮ projekto reguliavimo srityje. Lietuvos Respublikos krašto apsaugos ministerija numato parengti įgyvendinamąjį teisės aktą, kuriuo bus tvirtinamos kibernetinio saugumo rizikos valdymo priemonės.*	Dalinis
b) politiką dėl su kibernetiniu saugumu susijusių reikalavimų, taikomų IRT produktams ir IRT paslaugoms, įtraukimo ir specifikacijų viešuosiuose pirkimuose, įskaitant reikalavimus, susijusius su kibernetinio saugumo sertifikavimu, šifravimu ir atvirojo kodo kibernetinio saugumo produktų naudojimu;	**KSĮ projektas** **14 straipsnis. Kibernetinio saugumo rizikos valdymo priemonės** **1. Kibernetinio saugumo subjektai privalo užtikrinti šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus atitinkančiai veiklai vykdyti ar paslaugoms teikti naudojamų tinklų ir informacinių sistemų atitiktį kibernetinio saugumo rizikos valdymo priemonėms:**	Dalinis

	1) kibernetinio saugumo reikalavimams, tvirtinamiems Vyriausybės, išskyrus šio straipsnio 2 dalyje nurodytus atvejus; **2) Europos Komisijos priimtiems įgyvendinimo aktams, pagal šio straipsnio 3 dalyje nurodytas priemones nustatantiems techninius ir metodinius reikalavimus.** **<...>** **5. Kibernetinio saugumo reikalavimai apima šiuos elementus:** **<...>** **6) tinklų ir informacinių sistemų įsigijimą, plėtojimą ir priežiūros saugumą, įskaitant spragų valdymą ir atskleidimą.** *Platesnis Direktyvos 7 straipsnio 2 dalies b punkto įgyvendinimas nėra KSĮ projekto reguliavimo srityje. Lietuvos Respublikos krašto apsaugos ministerija numato parengti įgyvendinamąjį teisės aktą, kuriuo bus tvirtinamos kibernetinio saugumo rizikos valdymo priemonės.*	
c) pažeidžiamumų valdymo, apimančio koordinuoto pažeidžiamumų atskleidimo pagal 12 straipsnio 1 dalį skatinimą ir palengvinimą, politiką;	**KSĮ projektas** **14 straipsnis. Kibernetinio saugumo rizikos valdymo priemonės** **1. Kibernetinio saugumo subjektai privalo užtikrinti šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus atitinkančiai veiklai vykdyti ar paslaugoms teikti naudojamų tinklų ir informacinių sistemų atitiktį kibernetinio saugumo rizikos valdymo priemonėms:** **1) kibernetinio saugumo reikalavimams, tvirtinamiems Vyriausybės, išskyrus šio straipsnio 2 dalyje nurodytus atvejus;** **2) Europos Komisijos priimtiems įgyvendinimo aktams, pagal šio straipsnio 3 dalyje nurodytas priemones nustatantiems techninius ir metodinius reikalavimus.** **<...>** **5. Kibernetinio saugumo reikalavimai apima šiuos elementus:** **<..>** **6) tinklų ir informacinių sistemų įsigijimą, plėtojimą ir priežiūros saugumą, įskaitant spragų valdymą ir atskleidimą.** **KSĮ projektas** **25 straipsnis. Spragų paieška ir atskleidimas** **1. Spragų paieška ir atskleidimas laikomi teisėtais ir tokius veiksmus atlikusiam asmeniui neužtraukia teisinės atsakomybės tik tais atvejais, kai**	Visiškas

	spragų paieška atliekama kibernetinio saugumo subjektų valdomuose ir tvarkomuose tinkluose ir informacinėse sistemose laikantis šio straipsnio 2 dalyje, nacionalinės spragų atskleidimo tvarkos apraše, tvirtinamame krašto apsaugos ministro, ir (ar) kibernetinio saugumo subjekto nustatytos spragų atskleidimo tvarkos apraše, taip pat šio straipsnio 6 dalyje numatytų apribojimų. **2. Atliekant spragų paiešką laikomasi šių apribojimų:** **1) negali būti trikdomas ar keičiamas tinklų ir informacinės sistemos darbas, funkcionalumas, teikiamos paslaugos bei duomenų prieinamumas ar vientisumas;** **2) įsitikinus, kad spraga yra, nutraukiama spragos paieškos veikla, susijusi su aptikta spraga;** **3) subjektas, atlikęs spragų paiešką, ne vėliau kaip per 24 valandas nuo spragų paieškos pradžios (paiešką tęsiant ilgiau kaip 24 valandas – kas 24 valandas) turi parengti nacionalinės spragų atskleidimo tvarkos apraše ar kibernetinio saugumo subjekto nustatytos spragų atskleidimo tvarkos apraše nustatyto turinio informaciją apie spragų paieškos rezultatus ir ją pateikti Nacionaliniam kibernetinio saugumo centrui nacionalinės spragų atskleidimo tvarkos apraše nustatyta tvarka ir (ar) kibernetinio saugumo subjektui, kurio tinklų ir informacinėje sistemoje atlikta spragų paieška, šio kibernetinio saugumo subjekto nustatytos spragų atskleidimo tvarkos apraše nustatyta tvarka;** **4) nesiekiama be reikalo, daugiau, negu reikia spragai patvirtinti, stebėti, fiksuoti, perimti, įgyti, laikyti, atskleisti, kopijuoti, keisti, naikinti, gadinti, šalinti, naikinti kibernetinio saugumo subjekto valdomų ir (ar) tvarkomų duomenų;** **5) atskleidžiant spragą nenaudojami pastebėti, užfiksuoti, perimti, atskleisti asmens duomenys;** **6) nebandoma atspėti slaptažodžių, nenaudojami neteisėtu būdu gauti slaptažodžiai ir nėra manipuliuojama kibernetinio saugumo subjekto darbuotojais ar kitais asmenimis, turinčiais teisę naudotis viešai neskelbtina informacija, reikšminga spragų paieškai;** **7) nesidalijama informacija apie aptiktą spragą, išskyrus šios dalies 3 punkte ir šio straipsnio 6 dalyje nustatytus atvejus, taip pat kai informacija apie aptiktą spragą yra registruojama Europos pažeidžiamumų duomenų bazėje.** **3. Subjektas, surinkęs informaciją apie spragą, turi teisę šią informaciją anonimiškai pateikti Nacionaliniam kibernetinio saugumo centrui, išsaugodamas nacionalinės spragų atskleidimo tvarkos apraše nurodytą informaciją apie**	

	spragų paieškos rezultatų pateikimą. Nacionalinis kibernetinio saugumo centras užtikrina apie spragą pranešusio subjekto anonimišką. Šioje dalyje nurodytą informaciją apie spragų paieškos rezultatų pateikimą subjektas, surinkęs informaciją apie spragą, ir ją pateikęs anonimiškai, privalo saugoti 12 metų, nuo pranešimo Nacionaliniam kibernetinio saugumo centrui pateikimo dienos. **4. Spragų atskleidimo Nacionaliniam kibernetinio saugumo centrui tvarka, Nacionaliniam kibernetinio saugumo centrui teikiamos informacijos apie spragas turinys, trumpesnio negu 90 kalendorinių dienų informacijos apie aptiktą spragą atskleidimo kitiems, negu nurodyti šio straipsnio 2 dalies 3 punkte, asmenims termino nustatymo tvarka nustatomi nacionalinės spragų atkleidimo tvarkos apraše.** **5. Kibernetinio saugumo subjektas turi teisę nustatyti spragų jo valdomose ir (ar) tvarkomose tinklų ir informacinėse sistemose atskleidimo tvarką ir nustatyti kitus spragų paieškos apribojimus, negu numatyta šio straipsnio 2 dalyje, arba jų atsisakyti. Kibernetinio saugumo subjekto nustatytame spragų atskleidimo tvarkos apraše numatyti spragų paieškos apribojimai negali būti griežtesni, negu nurodyti šio straipsnio 2 dalyje. Kibernetinio saugumo subjekto nustatytame spragų atskleidimo tvarkos apraše negali būti nustatoma informacijos apie spragas pateikimo Nacionalinio kibernetinio saugumo centro tvarka ir numatomos šio straipsnio 6 dalyje nustatyto reguliavimo išimtys.** **6. Subjektas, nustatęs spragą, laikydamasis šio straipsnio 1 dalyje nurodytų apribojimų, turi teisę informaciją apie aptiktą spragą, tačiau ne daugiau, negu buvo pateikta Nacionaliniam kibernetinio saugumo centrui ir (ar) kibernetinio saugumo subjektui, atskleisti kitiems, negu nurodyti šio straipsnio 2 dalies 3 punkte, asmenims ne anksčiau kaip po 90 kalendorinių dienų nuo informacijos apie spragą pateikimo Nacionaliniam kibernetinio saugumo centrui ir (ar) kibernetinio saugumo subjektui. Nacionalinis kibernetinio saugumo centras, įvertinęs spragos sudėtingumą ir jos ištaisymo galimybes, nacionalinės spragų atskleidimo tvarkos apraše nustatyta tvarka turi teisę nustatyti trumpesnį informacijos apie aptiktą spragą atskleidimo kitiems, negu nurodyti šio straipsnio 2 dalies 3 punkte, asmenims terminą, tačiau ne trumpesnį kaip 3 kalendorinės dienos.**	
d) politiką, susijusią su bendru atvirojo interneto viešojo pagrindo prieinamumu, vientisumu ir konfidencialumu, įskaitant, kai tinkama, povandeninių ryšių kabelių kibernetinį saugumą;	**Lietuvos Respublikos elektroninių ryšių įstatymas** **4 straipsnis. Elektroninių ryšių politikos formavimo ir elektroninių ryšių veiklos reguliavimo institucijos**	Dalinis

	<...> 3. Elektroninių ryšių veiklą Lietuvos Respublikoje reguliuoja Ryšių reguliavimo tarnyba ir kitos valstybės institucijos pagal šiame įstatyme nustatytą kompetenciją. 4. Elektroninių ryšių, naudojamų valstybės gynybai, saugumui, viešajai tvarkai palaikyti, valstybės sienos apsaugai, laivybos saugumui, jūrų paieškos ir gelbėjimo darbams bei naftos išsiliejimų likvidavimo darbams vykdyti, civilinei aviacijai, traukinių eismo saugumui bei stabiliam ir patikimam energetikos sistemos darbui užtikrinti, veiklą pagal savo kompetenciją reguliuoja atitinkamos valstybės institucijos. Šių institucijų veiksmus, reguliuojant elektroninių ryšių veiklą, koordinuoja Susisiekimo ministerija. **9 straipsnis. Ryšių reguliavimo tarnybos, Tarybos ir jos pirmininko funkcijos** 1. Ryšių reguliavimo tarnyba: <...> 7) rengia pasiūlymus dėl elektroninių ryšių politikos formavimo ir juos teikia Susisiekimo ministerijai; *Platesnis Direktyvos 7 straipsnio 2 dalies d punkto įgyvendinimas nėra KSĮ projekto reguliavimo srityje. Lietuvos Respublikos krašto apsaugos ministerija numato parengti įgyvendinamąjį teisės aktą, kuriuo bus tvirtinamos kibernetinio saugumo rizikos valdymo priemonės.*	
e) atitinkamų pažangių technologijų, kuriomis siekiama įgyvendinti pažangiausias kibernetinio saugumo rizikos valdymo priemones, kūrimo ir integravimo skatinimo politiką;	**Pažangos priemonė** 7. Kibernetinio saugumo valdysenos stiprinimas 7.1. Kibernetinio saugumo valdysenos Lietuvoje stiprinimas (P-06-007-10-05-07-21 Sudarytos sąlygos kibernetinio saugumo subjektams nuosekliai didinti kibernetinio saugumo brandą, pasitelkiant visuotinai pripažintus ISO standartus (vnt.)). *Platesnis Direktyvos 7 straipsnio 2 dalies e punkto įgyvendinimas nėra KSĮ projekto reguliavimo srityje. Numatomas Nacionalinės kibernetinio saugumo plėtros programos tobulinimas.*	Dalinis
f) švietimo ir mokymo kibernetinio saugumo klausimais, kibernetinio saugumo įgūdžių, informuotumo didinimo ir mokslinių tyrimų ir technologinės plėtros iniciatyvų, taip pat	**NKSC nuostatai** 9. NKSC prie KAM veiklos tikslai:	Visiškas

gerosios kibernetinės higienos praktikos ir kontrolės gairių, skirtų piliečiams, suinteresuotiesiems subjektams ir kitiems subjektams, skatinimo ir plėtros politiką;	9.10. vykdyti 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamente (ES) Nr. 2021/887 (toliau – Reglamentas) nustatytas nacionalinio koordinavimo centro užduotis. <...> 16[3]. Įgyvendindamas 9.10 papunktyje nurodytą tikslą, NKSC prie KAM atlieka Reglamento 7 straipsnio 1 dalyje nustatytas užduotis. **Pažangos priemonė** 4. Žinių bei įgūdžių kibernetinio saugumo srityje plėtra 4.1. Kibernetinio saugumo subjektuose dirbančių darbuotojų, kibernetinio saugumo specialistų kompetencijų bei įgūdžių kibernetinio saugumo srityje stiprinimas bei pažeidžiamiausių visuomenės grupių kibernetinio saugumo brandos kėlimas (P-06-007-10-05-07-11 Parengta mokymo medžiaga, reikalinga kibernetinio saugumo kompetencijoms ugdyti (vnt.); P-06-007-10-05-07-03 Užbaigti kibernetinio saugumo mokymai (asm.); P-06-007-10-05-07-12 Kvalifikacijos kėlimo mokymuose dalyvavusių asmenų, dirbančių kibernetinio saugumo srityje, skaičius (asm.); P-06-007-10-05-07-13 Mokymuose dalyvavusių pažeidžiamiausių visuomenės grupių skaičius (vnt.); R-06-007-10-05-07-06 Švietimo ar mokymo veiklos dalyvių skaičius (asm.); R-06-007-10-05-07-07 Švietimo ar mokymo veiklos dalyvių skaičius: iš jų skaitmeninių įgūdžių ugdymo veiklos dalyvių skaičius (asm.) 7. Kibernetinio saugumo valdysenos stiprinimas 7.1. Kibernetinio saugumo valdysenos Lietuvoje stiprinimas (P-06-007-10-05-07-24 Komunikacijos kampanijų, skirtų visuomenės kibernetinio saugumo brandai didinti, sukūrimo ir sklaidos paslaugų skaičius (vnt.)). 8. Nacionalinio koordinavimo centro funkcijų vykdymas (P-06-007-10-05-07-05 Sukurta dinamiška ir aktyvi Lietuvos kibernetinio saugumo bendruomenė (asm.)).	
g) politiką dėl akademinių ir mokslinių tyrimų institucijų rėmimo siekiant kurti, tobulinti ir diegti kibernetinio saugumo priemones ir saugią tinklų infrastruktūrą;	**NKSC nuostatai** 9. NKSC prie KAM veiklos tikslai: 9.10. vykdyti 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamente (ES) Nr. 2021/887 (toliau – Reglamentas) nustatytas nacionalinio koordinavimo centro užduotis. <...> 16[3]. Įgyvendindamas 9.10 papunktyje nurodytą tikslą, NKSC prie KAM atlieka Reglamento 7 straipsnio 1 dalyje nustatytas užduotis. **Pažangos priemonė**	Visiškas

	7. Kibernetinio saugumo valdysenos stiprinimas 7.1. Kibernetinio saugumo valdysenos Lietuvoje stiprinimas (P-06-007-10-05-07-23 Parengtos viešojo ir privataus sektorių bendradarbiavimo vystymo kibernetinio saugumo srityje galimybių kryptys (vnt.)).	
h) politiką, įskaitant atitinkamas procedūras ir tinkamas dalijimosi informacija priemones, siekiant remti savanorišką dalijimąsi kibernetinio saugumo informacija tarp subjektų laikantis Sąjungos teisės;	**KSĮ projektas** **19 straipsnis. Kibernetinio saugumo informacinis tinklas** <...> **4. Kibernetinio saugumo subjektai turi teisę tapti Kibernetinio saugumo informacinio tinklo naudotojais, įgyvendindami tarpusavio dalijimosi kibernetinio saugumo informacija susitarimus. Nepriklausomai nuo to, ar naudojamasi Kibernetinio saugumo informaciniu tinklu, kibernetinio saugumo subjektai privalo pranešti Nacionaliniam kibernetinio saugumo centrui apie tokių susitarimų sudarymą, taip pat apie pasitraukimą iš tokių susitarimų per 20 darbo dienų nuo šių aplinkybių atsiradimo.** *Platesnis Direktyvos 7 straipsnio 2 dalies h punkto įgyvendinimas nėra KSĮ projekto reguliavimo srityje. Numatomas Kibernetinio saugumo informacinio tinklo tobulinimas.*	Dalinis
i) politiką, kuria stiprinami mažųjų ir vidutinių įmonių, visų pirma į šios direktyvos taikymo sritį nepatenkančių įmonių, kibernetinis atsparumas ir kibernetinės higienos bazinis lygis teikiant lengvai prieinamas gaires ir pagalbą jų konkretiems poreikiams tenkinti;	**Leidinys „Kibernetinis saugumas ir verslas“, 2020 m.** **Pažangos priemonė** 9. Kibernetinio saugumo atsparumo didinimas (P-06-007-10-05-07-04 Suteikta finansinė parama smulkaus ir vidutinio verslo subjektams kibernetiniam atsparumui stiprinti (vnt.)). *Platesnis Direktyvos 7 straipsnio 2 dalies i punkto įgyvendinimas nėra KSĮ projekto reguliavimo srityje. Numatomas Nacionalinės kibernetinio saugumo plėtros programos tobulinimas.*	Dalinis
j) politiką, kuria skatinama aktyvi kibernetinė apsauga.	**KSĮ projektas** **19 straipsnis. Kibernetinio saugumo informacinis tinklas** **1. Kibernetinio saugumo informacinis tinklas yra valstybės informacinė sistema, kurios paskirtis:** <...> **6) tvarkyti duomenis apie privalomus nurodymus blokuoti domeno vardą, identifikuojantį interneto svetainę ir juos viešai skelbti.**	Dalinis

	Platesnis Direktyvos 7 straipsnio 2 dalies j punkto įgyvendinimas nėra KSĮ projekto reguliavimo srityje. Lietuvos Respublikos krašto apsaugos ministerija numato parengti įgyvendinamąjį teisės aktą, kuriuo bus tvirtinamos kibernetinio saugumo rizikos valdymo priemonės.	
3. Valstybės narės per tris mėnesius nuo savo nacionalinių kibernetinio saugumo strategijų priėmimo apie jas praneša Komisijai. Valstybės narės į tokius pranešimus gali neįtraukti informacijos, kuri susijusi su jų nacionaliniu saugumu.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes ji jau įgyvendinta siekiant Nacionaliniame pažangos plano 1 priedo 10 tikslo „Stiprinti nacionalinį saugumą“ 10.5 uždavinio „Stiprinti kibernetinį saugumą ir gynybą“ bei patvirtinus Nacionalinio kibernetinio saugumo plėtros programą ir Pažangos priemonę.*	
4. Valstybės narės, remdamosi pagrindiniais veiklos rezultatų rodikliais, reguliariai ir bent kas penkerius metus vertina savo nacionalines kibernetinio saugumo strategijas ir prireikus jas atnaujina. ENISA valstybių narių prašymu padeda joms parengti arba atnaujinti nacionalinę kibernetinio saugumo strategiją ir pagrindinius veiklos rezultatų rodiklius, skirtus tai strategijai įvertinti, siekiant ją suderinti su šioje direktyvoje nustatytais reikalavimais ir pareigomis.	*Direktyvos 7 straipsnio 4 dalies įgyvendinimas nėra šio KSĮ projekto reguliavimo srityje.* *Direktyvos 7 straipsnio 4 dalis įgyvendinama vadovaujantis Lietuvos Respublikos strateginio valdymo įstatymu (suvestinė redakcija nuo 2024-01-01)).*	
8 straipsnis. Kompetentingos institucijos ir bendrieji kontaktiniai punktai		
1. Kiekviena valstybė narė paskiria arba įsteigia vieną arba daugiau kompetentingų institucijų, atsakingų už kibernetinį saugumą ir VII skyriuje nustatytų priežiūros užduočių vykdymą (toliau – kompetentingos institucijos).	**KSĮ projektas** **4 straipsnis. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos** <...> **3. Kibernetinio saugumo politiką įgyvendina Nacionalinis kibernetinio saugumo centras, Lietuvos policija ir Valstybinė duomenų apsaugos inspekcija.** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** <...> **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** <...> **16) atlieka kibernetinio saugumo subjektų atitikties kibernetinio saugumo rizikos valdymo priemonėms stebėseną;** **17) konsultuoja kibernetinio saugumo subjektus kibernetinio saugumo rizikos valdymo priemonių parinkimo ir taikymo klausimais;**	Visiškas
2. 1 dalyje nurodytos kompetentingos institucijos stebi šios direktyvos įgyvendinimą nacionaliniu lygmeniu.		

	<...> **20) atlieka kitas šiame įstatyme nustatytas funkcijas.** **26 straipsnis. Kibernetinio saugumo subjektų patikrinimai** **1. Nacionalinis kibernetinio saugumo centras atlieka kibernetinio saugumo subjektų atitikties šio įstatymo reikalavimams, išskyrus nustatytus šio įstatymo VI ir VII skyriuose, patikrinimus.**	
3. Kiekviena valstybė narė paskiria arba įsteigia bendrąjį kontaktinį punktą. Kai valstybė narė pagal 1 dalį paskiria arba įsteigia tik vieną kompetentingą instituciją, ta kompetentinga institucija taip pat laikoma tos valstybės narės bendruoju kontaktiniu punktu.	**KSĮ projektas** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** **<...>** **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** **18) bendradarbiauja su Europos Sąjungos, NATO ir kitų valstybių institucijomis ir organizacijomis, įgyvendinančiomis kibernetinio saugumo politiką, tarptautinėmis organizacijomis, turi teisę jas pasitelkti kartu atliekant šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje.**	Visiškas
4. Kiekvienas bendras kontaktinis punktas vykdo ryšių palaikymo funkciją, kad būtų užtikrintas jo valstybės narės institucijų tarpvalstybinis bendradarbiavimas su atitinkamomis kitų valstybių narių institucijomis ir, kai tinkama, Komisija bei ENISA, taip pat tarpsektorinis bendradarbiavimas su kitomis kompetentingomis institucijomis toje valstybėje narėje.	**KSĮ projektas** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** **<...>** **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** **18) bendradarbiauja su Europos Sąjungos, NATO ir kitų valstybių institucijomis ir organizacijomis, įgyvendinančiomis kibernetinio saugumo politiką, tarptautinėmis organizacijomis, turi teisę jas pasitelkti kartu atliekant šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje.**	Visiškas
5. Valstybės narės užtikrina, kad jų kompetentingos institucijos ir bendrieji kontaktiniai punktai turėtų tinkamų išteklių, kad veiksmingai ir efektyviai vykdytų jiems pavestas užduotis ir taip įgyvendintų šios direktyvos tikslus.	*Direktyvos 8 straipsnio 5 dalies įgyvendinimas nėra KSĮ projekto reguliavimo srityje.*	
6. Kiekviena valstybė narė nepagrįstai nedelsdama praneša Komisijai 1 dalyje nurodytos kompetentingos institucijos ir 3 dalyje nurodyto bendrojo kontaktinio punkto tapatybės duomenis, tų institucijų užduotis ir bet kokius vėlesnius jų pakeitimus. Kiekviena valstybė narė savo kompetentingos institucijos	Pranešimas Europos Komisijai pagal 8 str. įtrauktas į LINESIS priemonių planą.	

tapatybės duomenis paskelbia viešai. Komisija viešai paskelbia paskirtų bendrųjų kontaktinių punktų sąrašą.		
9 straipsnis. Nacionalinės kibernetinių krizių valdymo sistemos		
1. Kiekviena valstybė narė paskiria arba įsteigia vieną arba daugiau kompetentingų institucijų, kurios atsako už didelio masto kibernetinio saugumo incidentų ir krizių valdymą (toliau – kibernetinių krizių valdymo institucijos). Valstybės narės užtikrina, kad tos institucijos turėtų tinkamų išteklių, reikalingų veiksmingam ir efektyviam joms pavestų užduočių vykdymui. Valstybės narės užtikrina suderinamumą su esamomis nacionalinėmis bendro krizių valdymo sistemomis.	**KSĮ projektas** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** <...> **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** <...> **13) dalyvauja valdant krizes, susijusias su kibernetiniais incidentais, Krizių valdymo ir civilinės saugos įstatymo nustatyta tvarka;** **14) koordinuojant Nacionaliniam krizių valdymo centrui praneša Europos Sąjungos institucijoms apie šio straipsnio 2 dalies 13 punkte nurodytas krizes, kurių viena valstybė narė nepajėgia suvaldyti;** **KVĮ 42 straipsnis. Krizės valdymas.** **1. Vyriausybei priėmus sprendimą, kad būtina imtis krizės valdymo veiksmų, susidariusios krizės valdymą organizuoja ir koordinuoja Nacionalinis krizių valdymo centras.** **2. Krizės valdymas yra trijų lygmenų: strateginio, operacinio ir taktinio.** **3. Strateginiu lygmeniu Vyriausybė Nacionalinio saugumo komisijos siūlymu priima strateginius sprendimus dėl krizės valdymo.** **4. Operaciniu lygmeniu Nacionalinis krizių valdymo centras planuoja krizės valdymo priemones, koordinuoja ir kontroliuoja jų įgyvendinimą.** **5. Taktiniu lygmeniu veikia ministerijos ir kitos valstybės institucijos ir įstaigos, vykdydamos valstybiniuose krizių ir ekstremaliųjų situacijų valdymo planuose jų kompetencijai priskirtas ir ministerijos ir kitos valstybės institucijos ir įstaigos krizių ir ekstremaliųjų situacijų valdymo plane numatytas priemones, taip pat Vyriausybės joms skirtas valstybines reagavimo į krizes ir jų padarinių šalinimo užduotis.** **KVĮ įgyvendinantis teisės aktas** Pranešimo ir keitimosi informacija apie įvykį, ekstremalųjį įvykį, ypatingą įvykį, ekstremaliąją situaciją ar krizę tvarkos aprašas <...>	Visiškas

	8. Asmenys, atsakingi už informacijos teikimą, Informaciją teikia: 8.1. Nacionaliniam krizių valdymo centrui – informaciją apie kilusį ypatingą įvykį, nurodytą aprašo 1 priede; 9. Asmenys, atsakingi už informacijos teikimą, aprašo 8 punkte nustatytais atvejais nedelsdami telefonu ar kitomis ryšio priemonėmis teikia aprašo 1 priede nurodytų institucijų ir įstaigų bei aprašo 3 priede nurodytų atsakingųjų institucijų ir kitų informacijos teikėjų turimą pirminę Informaciją. Teikiant žvalgybos informaciją laikomasi Lietuvos Respublikos žvalgybos įstatyme nustatytų reikalavimų, o teikiant įslaptintą informaciją laikomasi Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatyme nustatytų reikalavimų. Pateikiami šie duomenys: 9.1. trumpas įvykio, ekstremaliojo įvykio, ypatingo įvykio, gresiančios, susidariusios ar paskelbtos ekstremaliosios situacijos, gręsiančios ar susidariusios krizės apibūdinimas (data, laikas, adresas, objektas, informacijos šaltinis, priežastys, prognozė), priimti sprendimai, planuojami ar atlikti pirminiai veiksmai; 9.2. esami ir galimi pavojaus gyventojų gyvybei ar sveikatai, jų būtiniausioms gyvenimo (veiklos) sąlygoms, turtui ir aplinkai, gyvybiškai svarbių valstybės funkcijų atlikimui, viešajai tvarkai šaltiniai, įvykio eigos prognozė; 9.3. ekstremaliosios situacijos operacijų vadovo pareigos, vardas, pavardė, telefonų numeriai (jeigu ekstremaliosios situacijos operacijų vadovas yra paskirtas); 9.4. gelbėjimo darbų vadovo pareigos, vardas, pavardė, telefonų numeriai.	
2. Jeigu valstybė narė paskiria arba įsteigia pagal 1 dalį daugiau nei vieną kibernetinių krizių valdymo instituciją, ji aiškiai nurodo, kuri iš tų institucijų yra koordinatorė valdant didelio masto kibernetinio saugumo incidentus ir krizes.	**KVĮ** **42 straipsnis. Krizės valdymas.** 1. Vyriausybei priėmus sprendimą, kad būtina imtis krizės valdymo veiksmų, susidariusios krizės valdymą organizuoja ir koordinuoja Nacionalinis krizių valdymo centras.	Visiškas
3. Kiekviena valstybė narė, taikydama šią direktyvą, nustato pajėgumus, objektus ir procedūras, kuriais galima pasinaudoti krizės atveju.	**KVĮ įgyvendinantis teisės aktas** <...> 6.1. Būtinų užduočių skyrimo, atlikimo ir kompensavimo už jų atlikimą tvarkos aprašas; (KVĮ 7 straipsnio 11 punktu, 39 straipsnio 1 ir 8 dalimis.) 6.2. Ekstremaliųjų situacijų operacijų centrų sudarymo, darbo organizavimo, sušaukimo tvarkos, uždavinių ir funkcijų tvarkos aprašas (KVĮ 7 straipsnio 21 punktu ir 15 straipsnio 4 dalimi); 6.3. Ekstremaliųjų situacijų skelbimo ir atšaukimo tvarkos aprašas (KVĮ 7 straipsnio 17 punktu, 32 straipsnio 5 dalimi); 6.4. Jungtinės grėsmių prevencijos ir krizių valdymo grupės uždavinių, funkcijų ir darbo organizavimo tvarkos aprašas (KVĮ 9 straipsnio 3 dalimi);	Visiškas

	6.5. Kriterijų, kuriuos atitinkančiuose ūkio subjektuose privaloma sudaryti ekstremaliųjų situacijų operacijų centrą, aprašas (KVĮ 15 straipsnio 2 dalimi); 6.6. Kriterijų, kuriuos atitinkančių kitų įstaigų ir ūkio subjektų vadovai privalo organizuoti ekstremaliųjų situacijų valdymo plano rengimą, aprašas (KVĮ 23 straipsnio 5 dalimi); 6.7. Krizių ir ekstremaliųjų situacijų prevencijos vykdymo tvarkos aprašas (KVĮ 20 straipsnio 5 dalimi); 6.8. Materialinių išteklių teikimo ir kompensavimo už jų teikimą tvarkos aprašas (KVĮ 7 straipsnio 13 punktu, 38 straipsnio 1 dalimi ir 48 straipsnio 2 dalimi); 6.9. Parengties pareigūnų funkcijoms ir valstybinei (valstybės perduotai savivaldybėms) civilinės saugos funkcijai atlikti reikalingų valstybės biudžeto lėšų poreikio nustatymo tvarkos aprašas (KVĮ 46 straipsnio 3 dalimi ir Lietuvos Respublikos biudžeto sandaros įstatymo 8 straipsnio 1 dalimi); 6.10. Pranešimo ir keitimosi informacija apie įvykį, ekstremalųjį įvykį, ypatingą įvykį, ekstremaliąją situaciją ar krizę tvarkos aprašas (KVĮ 7 straipsnio 12 ir 14 punktais); 6.11. Savanorių, tarptautinių humanitarinių organizacijų ir nevyriausybinių organizacijų pajėgų patirtų išlaidų kompensavimo sąlygų ir tvarkos aprašas (KVĮ 17 straipsnio 7 dalimi); 6.12. Slėptuvių, kolektyvinės apsaugos statinių ir priedangų poreikio nustatymo, parinkimo, žymėjimo, jų parengties organizavimo ir naudojimo tvarkos aprašas (KVĮ 7 straipsnio 20 punktu ir 28 straipsnio 7 dalimi); 6.13. Valstybės institucijų ir įstaigų, kurios rengia krizių ir ekstremaliųjų situacijų valdymo planus, sąrašas (KVĮ 7 straipsnio 23 punktu ir 23 straipsnio 3 dalimi; 6.14. Valstybės institucijų ir įstaigų, kuriose privaloma sudaryti ekstremaliųjų situacijų operacijų centrą, sąrašas (KVĮ 7 straipsnio 22 punktu ir 15 straipsnio 2 dalimi); 6.15. Valstybės ir savivaldybių institucijų ir įstaigų, kitų įstaigų, ūkio subjektų ir veiklos vykdytojų, kurie privalo kaupti jų nepertraukiamos veiklos vykdymui užtikrinti būtinas priemones ir asmenines apsaugos priemones, sąrašas (KVĮ 27 straipsnio 2 dalimi); 6.16. Valstybės ir savivaldybių institucijų ir įstaigų, kitų įstaigų, ūkio subjektų ir veiklos vykdytojų kaupiamų jų nepertraukiamos veiklos vykdymui užtikrinti būtinų priemonių ir asmeninių apsaugos priemonių sąrašo, kiekio ir laikotarpio nustatymo tvarkos aprašas (KVĮ 27 straipsnio 2 dalimi, Lietuvos Respublikos visuomenės	

	sveikatos priežiūros įstatymo 15 straipsnio 14 punktu ir Lietuvos Respublikos socialinių paslaugų įstatymo 23 straipsnio 1 dalies 1 punktu); 6.17. Valstybės paramos už žalą, patirtą dėl krizės ar ekstremaliosios situacijos, teikimo tvarkos aprašą (KVĮ 49 straipsniu ir atsižvelgiant į 2013 m. gruodžio 18 d. Komisijos reglamentą (ES) Nr. 1407/2013 dėl Sutarties dėl Europos Sąjungos veikimo 107 ir 108 straipsnių taikymo *de minimis* pagalbai, 2013 m. gruodžio 18 d. Komisijos reglamentą (ES) Nr. 1408/2013 dėl Sutarties dėl Europos Sąjungos veikimo 107 ir 108 straipsnių taikymo *de minimis* pagalbai žemės ūkio sektoriuje su paskutiniais pakeitimais, padarytais 2022 m. spalio 24 d. Komisijos reglamentu (ES) Nr. 2022/2046, 2014 m. birželio 27 d. Komisijos reglamentą (ES) Nr. 717/2014 dėl Sutarties dėl Europos Sąjungos veikimo 107 ir 108 straipsnių taikymo *de minimis* pagalbai žuvininkystės ir akvakultūros sektoriuje (toliau visi kartu – *de minimis* reglamentai)); 6.18. Krizių valdymo ir civilinės saugos mokymo tvarkos aprašas (KVĮ 7 straipsnio 15 punktu, 17 straipsnio 6 dalimi, 25 straipsnio 1 ir 2 dalimis).	
4. Kiekviena valstybė narė priima nacionalinį reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planą, kuriame išdėstomi didelio masto kibernetinio saugumo incidentų ir krizių valdymo tikslai ir tvarka. Tame plane visų pirma nustatomi: a) nacionalinių pasirengimo priemonių ir veiksmų tikslai;	**KVĮ** **21 straipsnis. Pasirengimo krizėms ir ekstremaliosioms situacijoms bendrosios nuostatos** 1. Krizėms ir ekstremaliosioms situacijoms rengiamasi siekiant užtikrinti įvykių, ekstremaliųjų įvykių likvidavimo, krizių ir ekstremaliųjų situacijų valdymo ir padarinių šalinimo, paieškos, gelbėjimo ir neatidėliotinus darbus ir gyvybiškai svarbių valstybės funkcijų atlikimą krizių ir ekstremaliųjų situacijų metu. 2. Pasirengimą krizėms sudaro: 1) krizių ir ekstremaliųjų situacijų valdymo planų rengimas; 2) perspėjimo sistemos parengtis; 3) krizių valdymo ir civilinės saugos mokymas ir gyventojų švietimas; 4) valstybinių pasirengimo krizėms užduočių skyrimas ir jų vykdymas; 5) valstybės institucijų ir įstaigų valstybės tarnautojų, darbuotojų, profesinės karo tarnybos karių, žvalgybos pareigūnų ir kitų asmenų pasitelkimas. 3. Pasirengimą ekstremaliosioms situacijoms sudaro: 1) ekstremaliųjų situacijų valdymo planų rengimas; 2) perspėjimo sistemos parengtis; 3) krizių valdymo ir civilinės saugos mokymas ir gyventojų švietimas; 4) valstybinių pasirengimo ekstremaliosioms situacijoms užduočių skyrimas ir jų vykdymas;	Visiškas

	5) slėptuvių, kolektyvinės apsaugos statinių ir priedangų poreikio nustatymas, parinkimas, žymėjimas ir jų parengties organizavimas; 6) valstybės institucijų ir įstaigų valstybės tarnautojų, darbuotojų, profesinės karo tarnybos karių, žvalgybos pareigūnų ir kitų asmenų pasitelkimas; 7) operacijų centrų sudarymas, patalpų ir darbo vietų įrengimas; 8) būtinų priemonių atsargų kaupimas; 9) materialinių išteklių teikimo sutarčių sudarymas ir administravimas; 10) pasirengimo ekstremaliosioms situacijoms vertinimas. **23 straipsnis. Krizių ir ekstremaliųjų situacijų valdymo planų rengimas** 1. Rengiami šie krizių ir ekstremaliųjų situacijų valdymo planai: 1) valstybiniai krizių ir ekstremaliųjų situacijų valdymo planai; 2) valstybės institucijų ir įstaigų krizių ir ekstremaliųjų situacijų valdymo planai; 3) kitų įstaigų ekstremaliųjų situacijų valdymo planai; 4) ūkio subjektų ir veiklos vykdytojų ekstremaliųjų situacijų valdymo planai; 5) savivaldybių ekstremaliųjų situacijų valdymo planai.	
b) kibernetinių krizių valdymo institucijų užduotys ir pareigos;	**KVĮ** **34 straipsnis. Valstybės lygio ekstremaliosios situacijos valdymas** 1. Gresiant ar susidarius valstybės lygio ekstremaliajai situacijai, Nacionalinis krizių valdymo centras: 1) vertina valstybės lygio ekstremaliosios situacijos grėsmę ir prireikus siūlo Vyriausybei skelbti valstybės lygio ekstremaliąją situaciją; 2) organizuoja gyventojų, valstybės ir savivaldybių institucijų ir įstaigų, kitų įstaigų, ūkio subjektų ir veiklos vykdytojų perspėjimą apie gresiančią ar susidariusią valstybės lygio ekstremaliąją situaciją; 3) renka informaciją apie gresiančią ar susidariusią valstybės lygio ekstremaliąją situaciją, rengia jos raidos prognozes ir planuoja tarpinstitucines priemones, siekdamas laiku reaguoti į galimas naujas grėsmes, vertina poreikį imtis krizės valdymo veiksmų; 4) išplatina valstybės institucijų ir įstaigų turimą arba joms skirtą informaciją, kuri leistų imtis priemonių, siekiant išvengti galimos žalos arba ją sušvelninti, arba koordinuoja valstybės institucijų ir įstaigų veiklą platinant tokią informaciją; 5) koordinuoja ir kontroliuoja valstybiniuose krizių ir ekstremaliųjų situacijų valdymo planuose numatytų priemonių įgyvendinimą valstybės mastu;	Visiškas

	6) kol paskiriamas valstybės operacijų vadovas, organizuoja ir koordinuoja neatidėliotinus darbus ir kitus veiksmus, būtinus valstybės lygio ekstremaliosios situacijos grėsmei likviduoti. 2. Gresiant ar susidarius valstybės lygio ekstremaliajai situacijai: 1) Priešgaisrinės apsaugos ir gelbėjimo departamentas perspėja gyventojus, valstybės ir savivaldybių institucijas ir įstaigas, kitas įstaigas, ūkio subjektus ir veiklos vykdytojus apie gresiančią ar susidariusią valstybės lygio ekstremaliąją situaciją, išplatina valstybės ir savivaldybių institucijų ir įstaigų turimą arba joms skirtą informaciją, kuri leistų imtis priemonių, siekiant išvengti galimos žalos arba ją sušvelninti; 2) Vyriausybė, atsižvelgdama į Nacionalinio krizių valdymo centro pasiūlymą ir įvykio, ekstremaliojo įvykio pobūdį, skelbia valstybės lygio ekstremaliąją situaciją ir paskiria valstybės operacijų vadovą. Valstybės operacijų vadovu skiriamas Vyriausybės narys, valstybės institucijos arba įstaigos, kurios veiklos srityje susidarė valstybės lygio ekstremalioji situacija, vadovas arba, kai valstybės lygio ekstremalioji situacija apima kelias valdymo (veiklos) sritis, valstybės operacijų vadovu gali būti skiriamas Nacionalinio krizių valdymo centro vadovas. 3. Gresiant ar susidarius valstybės lygio ekstremaliajai situacijai, taip pat ją paskelbus, ministerijos ar kitos valstybės institucijos ar įstaigos, kurioje sudarytas operacijų centras, vadovas ar jo įgaliotas asmuo nedelsdamas: 1) sušaukia ministerijos ar kitos valstybės institucijos ar įstaigos operacijų centrą; 2) organizuoja ministerijos ar kitos valstybės institucijos ar įstaigos valstybės tarnautojų ir darbuotojų, jų veiklos srities valstybės institucijų ir įstaigų perspėjimą apie gresiančią ar susidariusią ekstremaliąją situaciją; 3) išplatina informaciją, kuri leistų imtis priemonių, siekiant išvengti galimos žalos arba ją sušvelninti. 4. Gresiant ar susidarius valstybės lygio ekstremaliajai situacijai, taip pat ją paskelbus, ministerijos ar kitos valstybės institucijos ar įstaigos operacijų centras organizuoja ir koordinuoja ministerijos ar kitos valstybės institucijos ar įstaigos krizių ir ekstremaliųjų situacijų valdymo plane, valstybiniuose krizių ir ekstremaliųjų situacijų valdymo planuose ministerijai ar kitai valstybės institucijai ar įstaigai numatytų veiksmų ir priemonių įgyvendinimą, materialinių išteklių suteikimą, valstybės operacijų vadovo sprendimų vykdymą ir Nacionalinio krizių valdymo centro pasiūlymų ir šio centro vadovo pavedimų įgyvendinimą. 5. Paskelbus valstybės lygio ekstremaliąją situaciją:	

	1) Nacionalinis krizių valdymo centras: a) vykdo šio straipsnio 1 dalies 2–5 punktuose nustatytas funkcijas; b) padeda valstybės operacijų vadovui priimti sprendimus dėl valstybės lygio ekstremaliosios situacijos valdymo ir jos padarinių šalinimo organizavimo, teikia valstybės operacijų vadovui informaciją ir pasiūlymus dėl paieškos, gelbėjimo ir neatidėliotinų darbų, įvykių, ekstremaliųjų įvykių ir valstybės lygio ekstremaliosios situacijos valdymo ir jos padarinių šalinimo organizavimo darbų; c) koordinuoja ir kontroliuoja valstybės operacijų vadovo sprendimų įgyvendinimą; d) vertina papildomų materialinių ir žmogiškųjų išteklių, reikalingų valstybės lygio ekstremaliajai situacijai valdyti ir jos padariniams šalinti, poreikį, organizuoja ir koordinuoja šių išteklių skyrimą ir panaudojimą; 2) Vyriausybė gali nustatyti gyventojams, valstybės ir savivaldybių institucijoms ir įstaigoms, kitoms įstaigoms, ūkio subjektams ir veiklos vykdytojams asmens judėjimo laisvės, nuosavybės ir būsto neliečiamumo teisės, ūkinės veiklos laisvės, viešųjų ir administracinių paslaugų teikimo, streikų apribojimus valstybės lygio ekstremaliajai situacijai likviduoti ir jos padariniams šalinti; 3) atsiradus su valstybės lygio ekstremaliąja situacija susijusiam būtinų prekių ir (ar) paslaugų trūkumui ar ribotam prieinamumui, Vyriausybė imasi šių prekių tiekimą ir (ar) paslaugų teikimą ir prieinamumą didinančių priemonių; 4) krizių valdymo ir civilinės saugos sistemos subjektų prašymu Vyriausybė priima sprendimus dėl valstybės rezervo panaudojimo; 5) Vyriausybė skiria valstybės ir savivaldybių institucijoms ir įstaigoms valstybines reagavimo į ekstremaliąsias situacijas ir jų padarinių šalinimo užduotis; 6) valstybės operacijų vadovas atsako už neatidėliotinų darbų organizavimą, valstybės lygio ekstremaliosios situacijos valdymo ir jos padarinių šalinimo organizavimą; 7) savivaldybės operacijų centras organizuoja ir koordinuoja savivaldybės ekstremaliųjų situacijų valdymo plane, valstybiniuose krizių ir ekstremaliųjų situacijų valdymo planuose savivaldybei numatytų veiksmų ir priemonių įgyvendinimą, materialinių išteklių suteikimą, valstybės operacijų vadovo sprendimų vykdymą ir Nacionalinio krizių valdymo centro pasiūlymų ir šio centro vadovo pavedimų įgyvendinimą savivaldybės teritorijoje; 8) meras nedelsdamas sušaukia savivaldybės operacijų centrą, organizuoja valstybės tarnautojų ir darbuotojų perspėjimą apie gresiančią ar susidariusią valstybės lygio ekstremaliąją situaciją, išplatina savivaldybės teritorijoje informaciją, kuri leistų	

	imtis priemonių, siekiant išvengti galimos žalos arba ją sušvelninti, užtikrina Nacionalinio saugumo komisijos pasiūlymų, valstybės operacijų vadovo sprendimų ir Nacionalinio krizių valdymo centro vadovo pavedimų įgyvendinimą savivaldybės teritorijoje; 9) kiti krizių valdymo ir civilinės saugos sistemos subjektai vykdo savo ekstremaliųjų situacijų valdymo plane, krizių ir ekstremaliųjų situacijų valdymo plane ar valstybiniuose krizių ir ekstremaliųjų situacijų valdymo planuose pagal jų kompetenciją numatytas priemones ir veiksmus, užtikrina valstybės operacijų vadovo sprendimų ir Nacionalinio krizių valdymo centro vadovo pavedimų įgyvendinimą, organizuoja Nacionalinio krizių valdymo centro pasiūlymų įgyvendinimą. 6. Valstybės operacijų vadovas, atsižvelgdamas į valstybės lygio ekstremaliosios situacijos pobūdį, mastą ir jos valdymo rezultatus, jeigu šiame straipsnyje nustatytų priemonių taikymas nėra efektyvus ir neleidžia suvaldyti valstybės lygio ekstremaliosios situacijos ir (ar) pašalinti jos padarinių, gali motyvuotai kreiptis į Nacionalinį krizių valdymo centrą siūlydamas, kad būtų imtasi krizės valdymo veiksmų. 7. Ekstremaliųjų situacijų, apibrėžtų Nacionalinio saugumo strategijoje kaip keliančių ar galinčių sukelti grėsmę Lietuvos Respublikos nacionaliniam saugumui, valdymo koordinavimo klausimai gali būti svarstomi Nacionalinio saugumo komisijoje ar kitoje šiems klausimams svarstyti Vyriausybės sudarytoje komisijoje ar komitete. 8. Už Vyriausybės kompetencijai priskirtų sprendimų, būtinų valstybės lygio ekstremaliajai situacijai paskelbti, valdyti, jos padariniams šalinti, parengimą ir pateikimą Vyriausybei valstybės lygio ekstremaliosios situacijos metu yra atsakingas ministras, kuriam pavestose valdymo srityse yra susidariusi ar paskelbta valstybės lygio ekstremalioji situacija. **42 straipsnis. Krizės valdymas** 1. Vyriausybei priėmus sprendimą, kad būtina imtis krizės valdymo veiksmų, susidariusios krizės valdymą organizuoja ir koordinuoja Nacionalinis krizių valdymo centras. 2. Krizės valdymas yra trijų lygmenų: strateginio, operacinio ir taktinio. 3. Strateginiu lygmeniu Vyriausybė Nacionalinio saugumo komisijos siūlymu priima strateginius sprendimus dėl krizės valdymo. 4. Operaciniu lygmeniu Nacionalinis krizių valdymo centras planuoja krizės valdymo priemones, koordinuoja ir kontroliuoja jų įgyvendinimą.	

	5. Taktiniu lygmeniu veikia ministerijos ir kitos valstybės institucijos ir įstaigos, vykdydamos valstybiniuose krizių ir ekstremaliųjų situacijų valdymo planuose jų kompetencijai priskirtas ir ministerijos ir kitos valstybės institucijos ir įstaigos krizių ir ekstremaliųjų situacijų valdymo plane numatytas priemones, taip pat Vyriausybės joms skirtas valstybines reagavimo į krizes ir jų padarinių šalinimo užduotis. 6. Krizės metu Vyriausybė: 1) gali nustatyti gyventojams, valstybės ir savivaldybių institucijoms ir įstaigoms, kitoms įstaigoms, ūkio subjektams ir veiklos vykdytojams asmens judėjimo laisvės, nuosavybės ir būsto neliečiamumo teisės, ūkinės veiklos laisvės, viešųjų ir administracinių paslaugų teikimo apribojimus, būtinus krizei valdyti; 2) atsiradus su krize susijusiam būtinų prekių ir (ar) paslaugų trūkumui ar ribotam prieinamumui, Vyriausybė imasi šių prekių tiekimą ir (ar) paslaugų teikimą ir prieinamumą didinančių priemonių; 3) skiria valstybės ir savivaldybių institucijoms ir įstaigoms valstybines reagavimo į krizes ir jų padarinių šalinimo užduotis; 4) valstybės operacijų vadovu gali skirti Nacionalinio krizių valdymo centro vadovą; 5) priima kitus jos kompetencijai priskirtus sprendimus, būtinus krizei valdyti. 7. Krizės metu Nacionalinio saugumo komisija: 1) siūlo Vyriausybei priimti sprendimą, kad būtina imtis krizės valdymo veiksmų; 2) svarsto Nacionalinio krizių valdymo centro pasiūlymus dėl krizės valdymo prioritetų; 3) teikia Vyriausybei pasiūlymus dėl poreikio skirti valstybės ir savivaldybių institucijoms ir įstaigoms valstybines reagavimo į krizes ir jų padarinių šalinimo užduotis, taikyti šio straipsnio 6 dalies 1 ir 2 punktuose nurodytas priemones. 8. Krizės metu Nacionalinis krizių valdymo centras: 1) renka informaciją apie krizę, rengia jos raidos prognozes ir planuoja krizės valdymo priemones, teikia Nacionalinio saugumo komisijai pasiūlymus dėl krizės valdymo prioritetų, valstybinių reagavimo į krizes ir jų padarinių šalinimo užduočių skyrimo, teikia Vyriausybei pasiūlymus dėl kitų jos kompetencijai priskirtų sprendimų, būtinų krizei valdyti; 2) organizuoja ir koordinuoja krizės valdymą; 3) vertina papildomų materialinių ir žmogiškųjų išteklių poreikį krizei valdyti, organizuoja ir koordinuoja šių išteklių skyrimą ir panaudojimą.	

	9. Valstybės operacijų vadovas, krizės, kilusios dėl nesuvaldytos valstybės lygio ekstremaliosios situacijos, valdymo laikotarpiu priimamus sprendimus derina su Nacionaliniu krizių valdymo centru. Valstybės operacijų vadovo sprendimai, priimti nesuvaldytos valstybės lygio ekstremaliosios situacijos valdymo laikotarpiu (iki krizės pradžios), galioja, jeigu jie neprieštarauja sprendimams, kuriais reglamentuoti krizės valdymo veiksmai. Valstybės operacijų vadovas privalo pakeisti ar pripažinti netekusiais galios sprendimus, priimtus nesuvaldytos valstybės lygio ekstremaliosios situacijos valdymo laikotarpiu (iki krizės pradžios), jeigu jie prieštarauja sprendimams, kuriais reglamentuoti krizės valdymo veiksmai.	
c) kibernetinių krizių valdymo procedūros, įskaitant jų integravimą į nacionalinę bendro krizių valdymo sistemą, ir keitimosi informacija kanalai;	**KVĮ įgyvendinantis teisės aktas** <...> 6.1. Būtinų užduočių skyrimo, atlikimo ir kompensavimo už jų atlikimą tvarkos aprašas; (KVĮ 7 straipsnio 11 punktu, 39 straipsnio 1 ir 8 dalimis.) 6.2. Ekstremaliųjų situacijų operacijų centrų sudarymo, darbo organizavimo, sušaukimo tvarkos, uždavinių ir funkcijų tvarkos aprašas (KVĮ 7 straipsnio 21 punktu ir 15 straipsnio 4 dalimi); 6.3. Ekstremaliųjų situacijų skelbimo ir atšaukimo tvarkos aprašas (KVĮ 7 straipsnio 17 punktu, 32 straipsnio 5 dalimi); 6.4. Jungtinės grėsmių prevencijos ir krizių valdymo grupės uždavinių, funkcijų ir darbo organizavimo tvarkos aprašas (KVĮ 9 straipsnio 3 dalimi); 6.5. Kriterijų, kuriuos atitinkančiuose ūkio subjektuose privaloma sudaryti ekstremaliųjų situacijų operacijų centrą, aprašas (KVĮ 15 straipsnio 2 dalimi); 6.6. Kriterijų, kuriuos atitinkančių kitų įstaigų ir ūkio subjektų vadovai privalo organizuoti ekstremaliųjų situacijų valdymo plano rengimą, aprašas (KVĮ 23 straipsnio 5 dalimi); 6.7. Krizių ir ekstremaliųjų situacijų prevencijos vykdymo tvarkos aprašas (KVĮ 20 straipsnio 5 dalimi); 6.8. Materialinių išteklių teikimo ir kompensavimo už jų teikimą tvarkos aprašas (KVĮ 7 straipsnio 13 punktu, 38 straipsnio 1 dalimi ir 48 straipsnio 2 dalimi); 6.9. Parengties pareigūnų funkcijoms ir valstybinei (valstybės perduotai savivaldybėms) civilinės saugos funkcijai atlikti reikalingų valstybės biudžeto lėšų poreikio nustatymo tvarkos aprašas (KVĮ 46 straipsnio 3 dalimi ir Lietuvos Respublikos biudžeto sandaros įstatymo 8 straipsnio 1 dalimi);	Visiškas

	6.10. Pranešimo ir keitimosi informacija apie įvykį, ekstremalųjį įvykį, ypatingą įvykį, ekstremaliąją situaciją ar krizę tvarkos aprašas (KVĮ 7 straipsnio 12 ir 14 punktais); 6.11. Savanorių, tarptautinių humanitarinių organizacijų ir nevyriausybinių organizacijų pajėgų patirtų išlaidų kompensavimo sąlygų ir tvarkos aprašas (KVĮ 17 straipsnio 7 dalimi); 6.12. Slėptuvių, kolektyvinės apsaugos statinių ir priedangų poreikio nustatymo, parinkimo, žymėjimo, jų parengties organizavimo ir naudojimo tvarkos aprašas (KVĮ 7 straipsnio 20 punktu ir 28 straipsnio 7 dalimi); 6.13. Valstybės institucijų ir įstaigų, kurios rengia krizių ir ekstremaliųjų situacijų valdymo planus, sąrašas (KVĮ 7 straipsnio 23 punktu ir 23 straipsnio 3 dalimi; 6.14. Valstybės institucijų ir įstaigų, kuriose privaloma sudaryti ekstremaliųjų situacijų operacijų centrą, sąrašas (KVĮ 7 straipsnio 22 punktu ir 15 straipsnio 2 dalimi); 6.15. Valstybės ir savivaldybių institucijų ir įstaigų, kitų įstaigų, ūkio subjektų ir veiklos vykdytojų, kurie privalo kaupti jų nepertraukiamos veiklos vykdymui užtikrinti būtinas priemones ir asmenines apsaugos priemones, sąrašas (KVĮ 27 straipsnio 2 dalimi); 6.16. Valstybės ir savivaldybių institucijų ir įstaigų, kitų įstaigų, ūkio subjektų ir veiklos vykdytojų kaupiamų jų nepertraukiamos veiklos vykdymui užtikrinti būtinų priemonių ir asmeninių apsaugos priemonių sąrašo, kiekio ir laikotarpio nustatymo tvarkos aprašas (KVĮ 27 straipsnio 2 dalimi, Lietuvos Respublikos visuomenės sveikatos priežiūros įstatymo 15 straipsnio 14 punktu ir Lietuvos Respublikos socialinių paslaugų įstatymo 23 straipsnio 1 dalies 1 punktu); 6.17. Valstybės paramos už žalą, patirtą dėl krizės ar ekstremaliosios situacijos, teikimo tvarkos aprašą (KVĮ 49 straipsniu ir atsižvelgiant į 2013 m. gruodžio 18 d. Komisijos reglamentą (ES) Nr. 1407/2013 dėl Sutarties dėl Europos Sąjungos veikimo 107 ir 108 straipsnių taikymo *de minimis* pagalbai, 2013 m. gruodžio 18 d. Komisijos reglamentą (ES) Nr. 1408/2013 dėl Sutarties dėl Europos Sąjungos veikimo 107 ir 108 straipsnių taikymo *de minimis* pagalbai žemės ūkio sektoriuje su paskutiniais pakeitimais, padarytais 2022 m. spalio 24 d. Komisijos reglamentu (ES) Nr. 2022/2046, 2014 m. birželio 27 d. Komisijos reglamentą (ES) Nr. 717/2014 dėl Sutarties dėl Europos Sąjungos veikimo 107 ir 108 straipsnių taikymo *de minimis* pagalbai žuvininkystės ir akvakultūros sektoriuje (toliau visi kartu – *de minimis* reglamentai)); 	

	6.18. Krizių valdymo ir civilinės saugos mokymo tvarkos aprašas (KVĮ 7 straipsnio 15 punktu, 17 straipsnio 6 dalimi, 25 straipsnio 1 ir 2 dalimis).	
d) nacionalinės pasirengimo priemonės, įskaitant pratybas ir mokymo veiklą;	**KVĮ** **21 straipsnis. Pasirengimo krizėms ir ekstremaliosioms situacijoms bendrosios nuostatos** 1. Krizėms ir ekstremaliosioms situacijoms rengiamasi siekiant užtikrinti įvykių, ekstremaliųjų įvykių likvidavimo, krizių ir ekstremaliųjų situacijų valdymo ir padarinių šalinimo, paieškos, gelbėjimo ir neatidėliotinus darbus ir gyvybiškai svarbių valstybės funkcijų atlikimą krizių ir ekstremaliųjų situacijų metu. 2. Pasirengimą krizėms sudaro: 1) krizių ir ekstremaliųjų situacijų valdymo planų rengimas; 2) perspėjimo sistemos parengtis; 3) krizių valdymo ir civilinės saugos mokymas ir gyventojų švietimas; 4) valstybinių pasirengimo krizėms užduočių skyrimas ir jų vykdymas; 5) valstybės institucijų ir įstaigų valstybės tarnautojų, darbuotojų, profesinės karo tarnybos karių, žvalgybos pareigūnų ir kitų asmenų pasitelkimas. 3. Pasirengimą ekstremaliosioms situacijoms sudaro: 1) ekstremaliųjų situacijų valdymo planų rengimas; 2) perspėjimo sistemos parengtis; 3) krizių valdymo ir civilinės saugos mokymas ir gyventojų švietimas; 4) valstybinių pasirengimo ekstremaliosioms situacijoms užduočių skyrimas ir jų vykdymas; 5) slėptuvių, kolektyvinės apsaugos statinių ir priedangų poreikio nustatymas, parinkimas, žymėjimas ir jų parengties organizavimas; 6) valstybės institucijų ir įstaigų valstybės tarnautojų, darbuotojų, profesinės karo tarnybos karių, žvalgybos pareigūnų ir kitų asmenų pasitelkimas; 7) operacijų centrų sudarymas, patalpų ir darbo vietų įrengimas; 8) būtinų priemonių atsargų kaupimas; 9) materialinių išteklių teikimo sutarčių sudarymas ir administravimas; 10) pasirengimo ekstremaliosioms situacijoms vertinimas. **25 straipsnis. Krizių valdymo ir civilinės saugos mokymas ir gyventojų švietimas** 1. Siekdamos pasirengti įvykių, ekstremaliųjų įvykių likvidavimui, krizių ir ekstremaliųjų situacijų valdymui, jų padarinių šalinimui, paieškos, gelbėjimo ir neatidėliotiniems darbams ir gyvybiškai svarbių valstybės funkcijų atlikimui krizių ir ekstremaliųjų situacijų metu, valstybės ir savivaldybių institucijos ir įstaigos, kitos	Visiškas

	įstaigos, ūkio subjektai ir veiklos vykdytojai Vyriausybės nustatyta tvarka organizuoja krizių valdymo ir civilinės saugos mokymą, į kurį yra integruotas pasirengimo karinėms ir hibridinėms grėsmėms mokymo turinys. 2. Valstybės ir savivaldybių institucijų ir įstaigų, kitų įstaigų, ūkio subjektų ir veiklos vykdytojų vadovai privalo siųsti Vyriausybės nustatytų kategorijų asmenis, dirbančius jų vadovaujamose valstybės ir savivaldybių institucijose ir įstaigose, kitose įstaigose, ūkio subjektuose, išklausyti Priešgaisrinės apsaugos ir gelbėjimo departamento direktoriaus patvirtintos civilinės saugos mokymo programos kurso. Šie asmenys mokomi ir jų kvalifikacija civilinės saugos srityje tobulinama Vyriausybės nustatyta tvarka. 3. Krizių valdymo ir civilinės saugos mokymas vykdomas ikimokyklinio, priešmokyklinio ir (ar) bendrojo ugdymo ir profesinio mokymo įstaigose pagal švietimo, mokslo ir sporto ministro tvirtinamas bendrąsias programas, kriterijus ar gaires, į kurias yra integruotas su Priešgaisrinės apsaugos ir gelbėjimo departamentu suderintas mokymo turinys, nurodytas šio straipsnio 1 dalyje. Krizių valdymo ir civilinės saugos mokymas aukštosiose mokyklose vykdomas aukštosios mokyklos nustatyta tvarka. 4. Gyventojų švietimas civilinės saugos klausimais vykdomas Priešgaisrinės apsaugos ir gelbėjimo departamento direktoriaus nustatyta tvarka. Priešgaisrinės apsaugos ir gelbėjimo departamentas koordinuoja gyventojų švietimą civilinės saugos klausimais, teikia savivaldybės administracijos direktoriui metodinę pagalbą. Gyventojų švietimas turi būti atliekamas asmenims su negalia pritaikytais bendravimo būdais (pavyzdžiui, žodiniu, rašytiniu, garsiniu ir (ar) vaizdiniu informacijos perdavimo ir (ar) gavimo būdais naudojant Brailio raštą, multimedijos priemones, garsines priemones, lengvai suprantamą (paprastą ir aiškiai struktūrizuotą) kalbą, gestų kalbą, taip pat patobulintus ir (ar) alternatyvius bendravimo būdus, priemones ir formas, informacijos ir ryšių technologijas, kuriomis disponuojama). **26 straipsnis. Krizių valdymo ir civilinės saugos pratybos** 1. Krizių valdymo ir civilinės saugos pratybos yra krizių valdymo ir civilinės saugos mokymo dalis. 2. Valstybės ir savivaldybių institucijų ir įstaigų, kitų įstaigų, ūkio subjektų, veiklos vykdytojų ir savanorių ir NVO pajėgų pasirengimas patikrinamas krizių valdymo ir (ar) civilinės saugos pratybose, kai tariamomis ekstremaliosios situacijos ar krizės sąlygomis tikrinami veiksmai ir procedūros, numatytos ekstremaliųjų situacijų valdymo planuose ar krizių ir ekstremaliųjų situacijų valdymo planuose,	

	tobulinami sprendimų priėmimo įgūdžiai, mokomasi praktiškai organizuoti ir atlikti krizių valdymą, paieškos, gelbėjimo ir neatidėliotinus darbus, likviduoti įvykius, ekstremaliuosius įvykius, krizes ar ekstremaliąsias situacijas ir šalinti jų padarinius. 3. Ministerijos ir kitos valstybės institucijos ir įstaigos pagal kompetenciją organizuoja civilinės saugos pratybas, dalyvauja šio straipsnio 9 dalyje nurodytose pratybose. 4. Savivaldybės administracijos direktorius: 1) organizuoja savivaldybės lygio civilinės saugos pratybas; 2) užtikrina savivaldybės įstaigų ir viešųjų įstaigų, kurių savininkė yra savivaldybė, ir savivaldybės valdomų įmonių dalyvavimą pagal jų kompetenciją (veiklos sritį) valstybės lygio krizių valdymo ir civilinės saugos pratybose. 5. Ūkio subjekto, kitos įstaigos ir veiklos vykdytojo vadovas arba jo įgaliotas asmuo organizuoja ūkio subjekto, kitos įstaigos ir veiklos vykdytojo darbuotojų civilinės saugos pratybas. 6. Priešgaisrinės apsaugos ir gelbėjimo departamentas ir jam pavaldžios įstaigos pagal kompetenciją organizuoja civilinės saugos pratybas, koordinuoja civilinės saugos pratybų organizavimą savivaldybėse, valstybės ir savivaldybių institucijoms ir įstaigoms teikia metodinę pagalbą civilinės saugos pratybų organizavimo klausimais. 7. Priešgaisrinės apsaugos ir gelbėjimo departamento direktorius tvirtina civilinės saugos pratybų organizavimo ir vertinimo metodines rekomendacijas. 8. Vidaus reikalų ministras tvirtina valstybės lygio civilinės saugos pratybų planus. Valstybės lygio civilinės saugos pratybas organizuoja vidaus reikalų ministro tvirtinamuose valstybės lygio civilinės saugos pratybų planuose nurodytos valstybės institucijos ir įstaigos. 9. Valstybės ir tarptautinio lygio krizių valdymo pratybas organizuoja Nacionalinis krizių valdymo centras. 10. Krizių valdymo ir civilinės saugos pratybos organizuojamos Vyriausybės nustatyta tvarka.	
e) atitinkami viešieji ir privatieji suinteresuotieji subjektai ir naudojama infrastruktūra;	**KVĮ įgyvendinantis teisės aktas** <...> 6.1. Būtinų užduočių skyrimo, atlikimo ir kompensavimo už jų atlikimą tvarkos aprašas; 6.4. Jungtinės grėsmių prevencijos ir krizių valdymo grupės uždavinių, funkcijų ir darbo organizavimo tvarkos aprašas;	Visiškas

	6.8. Materialinių išteklių teikimo ir kompensavimo už jų teikimą tvarkos aprašas.	
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.	**KSĮ projektas** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** **<...>** **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** **<...>** **13) dalyvauja valdant krizes, susijusias su kibernetiniais incidentais, Krizių valdymo ir civilinės saugos įstatymo nustatyta tvarka;** **14) koordinuojant Nacionaliniam krizių valdymo centrui praneša Europos Sąjungos institucijoms apie šio straipsnio 2 dalies 13 punkte nurodytas krizes, kurių viena valstybė narė nepajėgia suvaldyti;** **KVĮ** **50 straipsnis. Tarptautinis bendradarbiavimas krizių valdymo ir civilinės saugos srityje** **<...>** **4. Nacionalinis krizių valdymo centras koordinuoja tarptautinį bendradarbiavimą krizių valdymo srityje, konsultuoja Lietuvos Respublikos užsienio reikalų ministeriją ir teikia pagalbą diplomatinei tarnybai atstovaujant Lietuvos Respublikos interesams tarptautinėse institucijose ir organizacijose, teikiant informaciją Lietuvoje akredituotų užsienio valstybių diplomatinėms atstovybėms, Europos Sąjungos įstaigoms, tarptautinių organizacijų atstovybėms, kitoms atstovybėms, akredituotiems jų nariams.** **5. Nacionalinis krizių valdymo centras, bendradarbiaudamas su Užsienio reikalų ministerija ir Lietuvos Respublikos krašto apsaugos ministerija, vykdo nacionalinių krizių valdymo procedūrų atitikties NATO ir Europos Sąjungos institucijų nustatytoms procedūroms priežiūrą.**	Visiškas
5. Per tris mėnesius nuo 1 dalyje nurodytos kibernetinių krizių valdymo institucijos paskyrimo arba įsteigimo kiekviena valstybė narė praneša Komisijai apie savo institucijos tapatybės duomenis ir apie visus vėlesnius jos pakeitimus. Valstybės narės pateikia Komisijai ir Europos ryšių palaikymo dėl kibernetinių krizių organizacinio tinklui (EU-CyCLONe) atitinkamą informaciją, susijusią su 4 dalies reikalavimais, apie savo nacionalinius	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes ji jau įgyvendinta KVĮ.*	

reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planus per tris mėnesius nuo tų planų priėmimo. Valstybės narės gali nenurodyti konkrečios informacijos, jeigu tai yra būtina jų nacionaliniam saugumui ir tik tokiam saugumui būtinu mastu.		
10 straipsnis. Reagavimo į kompiuterių saugumo incidentus tarnybos (CSIRT)		
1. Kiekviena valstybė narė paskiria arba įsteigia vieną arba daugiau CSIRT. CSIRT gali būti paskirtos arba įsteigtos kompetentingoje institucijoje. CSIRT laikosi 11 straipsnio 1 dalyje išdėstytų reikalavimų, apima bent I ir II prieduose nurodytus sektorius, subsektorius ir subjektų rūšis ir atsako už incidentų valdymą pagal aiškiai apibrėžtą procesą.	**KSĮ projektas** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** **<...>** **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** **<...>** **3) valdo kibernetinius incidentus nacionalinio kibernetinių incidentų valdymo plano, tvirtinamo Vyriausybės, nustatyta tvarka;**	Visiškas
2. Valstybės narės užtikrina, kad kiekviena CSIRT turėtų tinkamų išteklių, kad galėtų veiksmingai vykdyti savo užduotis, nurodytas 11 straipsnio 3 dalyje.	*Direktyvos 10 straipsnio 2 dalies įgyvendinimas nėra KSĮ projekto reguliavimo srityje.*	
3. Valstybės narės užtikrina, kad kiekviena CSIRT turėtų tinkamą, saugią ir atsparią ryšių ir informacinę struktūrą, kuria naudodamosi jos galėtų keistis informacija su esminiais ir svarbiais subjektais ir kitais atitinkamais suinteresuotaisiais subjektais. Tuo tikslu valstybės narės užtikrina, kad kiekviena CSIRT prisidėtų prie saugaus dalijimosi informacija priemonių diegimo.	**KSĮ projektas** **19 straipsnis. Kibernetinio saugumo informacinis tinklas** **1. Kibernetinio saugumo informacinis tinklas yra valstybės informacinė sistema, kurios paskirtis:** **1) registruoti Kibernetinio saugumo subjektų registro objektus ir tvarkyti jų duomenis;** **2) tvarkyti duomenis, surinktus techninėmis kibernetinio saugumo priemonėmis, siekiant užkardyti ir valdyti kibernetinius incidentus;** **3) tvarkyti duomenis, susijusius su kibernetinio saugumo rizikos valdymo priemonių įgyvendinimo stebėsena;** **4) tvarkyti duomenis apie kibernetinio saugumo subjektus, kitas įstaigas ir ūkio subjektus, kuriems, įvykus ekstremaliajam įvykiui kibernetinėje erdvėje, būtų pavedamos būtinosios užduotys valdant kibernetinius incidentus;** **5) keistis su Kibernetinio saugumo informacinio tinklo naudotojais duomenimis, susijusiais su kibernetiniais incidentais, kibernetinėmis grėsmėmis, vos neįvykusiais kibernetiniais incidentais, taip pat kita su kibernetinio saugumo užtikrinimu susijusia informacija;**	Visiškas

	6) tvarkyti duomenis apie privalomus nurodymus blokuoti domeno vardą, identifikuojantį interneto svetainę ir juos viešai skelbti. **7) teikti kibernetinio saugumo paslaugas ir priemones, įskaitant mokymų ir pratybų paslaugas ir įrankius.** **16 straipsnis. Techninės kibernetinio saugumo priemonės** **1. Vykdydamas esminių subjektų valdomų ir (ar) tvarkomų tinklų ir informacinių sistemų stebėseną, siekdamas realiu laiku arba beveik realiu laiku identifikuoti kibernetines grėsmes ir kibernetinius incidentus, Nacionalinis kibernetinio saugumo centras esminių subjektų tinklų ir informacinėse sistemose diegia ir valdo technines kibernetinio saugumo priemones. Svarbių subjektų valdomose ir (ar) tvarkomose tinklų ir informacinėse sistemose techninės kibernetinio saugumo priemonės gali būti diegiamos jų prašymu, siekiant suvaldyti kibernetinius incidentus. Šioje dalyje numatytų priemonių diegimas ir naudojimas atliekamas taip, kad būtų užtikrinamas kibernetinio saugumo subjektų valdomų ir (ar) tvarkomų tinklų ir informacinės sistemos nepertraukiamas veikimas.**	
4. CSIRT pagal 29 straipsnį bendradarbiauja ir, kai tinkama, keičiasi atitinkama informacija su sektoriaus arba kelių sektorių esminių ir svarbių subjektų bendruomenėmis.	**KSĮ projektas** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** **<...>** **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** **<...>** **4) realiuoju laiku arba beveik realiuoju laiku kibernetinio saugumo subjektams ir suinteresuotiesiems asmenims teikia ankstyvuosius perspėjimus, įspėjimus, pranešimus ir keičiasi informacija apie kibernetines grėsmes, spragas, kibernetinius incidentus ir vos neįvykusius kibernetinius incidentus;** **<...>** **18) bendradarbiauja su Europos Sąjungos, NATO ir kitų valstybių institucijomis ir organizacijomis, įgyvendinančiomis kibernetinio saugumo politiką, tarptautinėmis organizacijomis, turi teisę jas pasitelkti kartu atliekant šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje;** **19) kartu su verslo subjektais, mokslo ir studijų institucijomis, nacionalinėmis, Europos Sąjungos, NATO ir kitų valstybių institucijomis ir organizacijomis, tarptautinėmis organizacijomis, nevyriausybinėmis**	Visiškas

	organizacijomis bei kibernetinio saugumo subjektais plėtoja nacionalinį kibernetinį saugumą stiprinančius projektus;	
5. CSIRT dalyvauja tarpusavio vertinimuose, kurie organizuojami pagal 19 straipsnį.	**KSĮ projektas** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** **<...>** **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** **<...>** **18) bendradarbiauja su Europos Sąjungos, NATO ir kitų valstybių institucijomis ir organizacijomis, įgyvendinančiomis kibernetinio saugumo politiką, tarptautinėmis organizacijomis, turi teisę jas pasitelkti kartu atliekant šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje;**	Visiškas
6. Valstybės narės užtikrina efektyvų, veiksmingą ir saugų jų CSIRT bendradarbiavimą CSIRT tinkle.	**KSĮ projektas** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** **<...>** **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** **<...>** **15) dalyvauja Europos Sąjungos ir NATO įsteigtų reagavimo į kibernetinius incidentus tinklų veikloje ir teikia savitarpio pagalbą pagal savo pajėgumus ir kompetenciją kitiems šių tinklų nariams jų prašymu.**	Visiškas
7. CSIRT gali užmegzti bendradarbiavimo ryšius su trečiųjų valstybių nacionalinėmis reagavimo į kompiuterių saugumo incidentus grupėmis. Palaikydamos tokius bendradarbiavimo santykius, valstybės narės sudaro palankesnes sąlygas veiksmingai, efektyviai ir saugiai keistis informacija su tomis trečiųjų valstybių nacionalinėmis reagavimo į kompiuterių saugumo incidentus grupėmis, naudodamos atitinkamus dalijimosi informacija protokolus, įskaitant Srauto kontrolės protokolą. CSIRT gali keistis atitinkama informacija su trečiųjų valstybių nacionalinėmis reagavimo į kompiuterių saugumo incidentus grupėmis, įskaitant asmens duomenis, laikydamosi Sąjungos duomenų apsaugos teisės.	**KSĮ projektas** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** **<...>** **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** **<...>** **18) bendradarbiauja su Europos Sąjungos, NATO ir kitų valstybių institucijomis ir organizacijomis, įgyvendinančiomis kibernetinio saugumo politiką, tarptautinėmis organizacijomis, turi teisę jas pasitelkti kartu atliekant šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje;** **22 straipsnis. Informacijos, tvarkomos tarpinstitucinio bendradarbiavimo metu, apsauga**	Visiškas
8. CSIRT gali bendradarbiauti su trečiųjų valstybių nacionalinėmis reagavimo į kompiuterių saugumo incidentus		

grupėmis arba lygiavertėmis trečiųjų valstybių įstaigomis, visų pirma siekdamos teikti joms pagalbą kibernetinio saugumo srityje.	**1. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos šio įstatymo tikslais gauta informacija, įskaitant asmens duomenis ir konfidencialią informaciją, turi teisę keistis tarpusavyje, su kitų valstybių institucijomis, NATO ir Europos Sąjungos institucijomis ir tarptautinėmis organizacijomis tik tiek, kiek tai yra būtina šių institucijų funkcijoms pagal kompetenciją atlikti, atsižvelgiant į keitimosi informacija tikslą ir proporcingumą.** **2. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos, tvarkydamos šio įstatymo tikslais gautą informaciją, saugo įslaptintą informaciją, asmenų saugumo ir komercinius interesus, taip pat pateiktos informacijos konfidencialumą. Šioje dalyje nurodyta informacija teikiama tik tais atvejais, jeigu teisė gauti šią informaciją yra nustatyta įstatymuose ar jų pagrindu priimtuose kituose įgyvendinamuosiuose norminiuose teisės aktuose.** **3. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos šio įstatymo tikslais tvarkomus asmens duomenis tvarko laikydamosi Asmens duomenų teisinės apsaugos įstatymo, Reglamento (ES) 2016/679 ir Asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymu.**	
9. Kiekviena valstybė narė nepagrįstai nedelsdama praneša Komisijai šio straipsnio 1 dalyje nurodytos CSIRT ir CSIRT, paskirtos koordinatore pagal 12 straipsnio 1 dalį, tapatybės duomenis, jų atitinkamas užduotis, kurias jos vykdo esminių ir svarbių subjektų atžvilgiu, ir bet kokius vėlesnius jų pakeitimus.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes Nacionalinis kibernetinio saugumo centras CSIRT funkcijas jau vykdo pagal Lietuvos Respublikos kibernetinio saugumo įstatymą (suvestinė redakcija (2024-01-01 - 2024-04-30)).*	
10. Valstybės narės gali paprašyti ENISA padėti kurti jų CSIRT.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
11 straipsnis. CSIRT keliami reikalavimai, techniniai pajėgumai ir užduotys		
1. CSIRT turi atitikti šiuos reikalavimus: a) CSIRT užtikrina, kad jų ryšio kanalai būtų lengvai prieinami išvengiant kritinių funkcionavimo trikties taškų, taip pat nustato keletą būdų, kaip bet kuriuo metu susisiekti su jomis ir su kitais subjektais; jos aiškiai nurodo ryšių kanalus ir apie juos informuoja savo klientus ir bendradarbiavimo partnerius;	**KSĮ projektas** **5. Nacionalinis kibernetinio saugumo centras turi atitikti šiuos reikalavimus:** **1) Nacionalinio kibernetinio saugumo centro ryšio kanalai turi būti lengvai prieinami išvengiant kritinių funkcionavimo trikties taškų,** **2) turi būti nustatoma keletas būdų, kaip bet kuriuo metu susisiekti su Nacionaliniu kibernetinio saugumo centru ir su kitais subjektais, apie šiuos**	Visiškas

b) CSIRT biurai ir pagalbinės informacinės sistemos turi būti saugiose vietose; c) CSIRT aprūpinamos tinkama prašymų valdymo ir nukreipimo sistema, visų pirma siekiant palengvinti veiksmingą ir efektyvų perdavimą; d) CSIRT užtikrina savo veiklos konfidencialumą ir patikimumą; e) CSIRT turi turėti pakankamai darbuotojų, kad būtų užtikrintas pasiekiamumas bet kuriuo metu, ir jos turi užtikrinti tinkamą savo darbuotojų mokymą; f) CSIRT aprūpinamos antrinėmis sistemomis ir atsargine darbo erdve, kad būtų užtikrintas jų paslaugų tęstinumas; CSIRT gali dalyvauti tarptautiniuose bendradarbiavimo tinkluose.	**būdus ir ryšių kanalus informuojant kibernetinio saugumo subjektus ir kitas šio įstatymo 20 straipsnyje nurodytas institucijas;** **3) Nacionalinio kibernetinio saugumo centro patalpos ir pagalbinės informacinės sistemos turi būti saugiose vietose;** **4) Nacionalinis kibernetinio saugumo centras turi turėti prašymų valdymo ir nukreipimo sistemą, užtikrinančią veiksmingą ir efektyvų prašymų perdavimą;** **5) Nacionalinis kibernetinio saugumo centras privalo užtikrinti savo veiklos konfidencialumą ir patikimumą;** **6) Nacionalinis kibernetinio saugumo centras privalo turėti pakankamai darbuotojų, kad būtų užtikrintas Nacionalinio kibernetinio saugumo centro pasiekiamumas bet kuriuo metu,** **7) Nacionalinio kibernetinio saugumo centro darbuotojai turi būti tinkamai apmokyti jų vykdomoms funkcijoms;** **8) Nacionalinis kibernetinio saugumo centras turi turėti antrines sistemas ir atsarginę darbo erdvę, kad būtų užtikrintas Nacionalinis kibernetinio saugumo centro funkcijų tęstinumas.**	
2. Valstybės narės užtikrina, kad jų CSIRT bendrai turėtų techninių pajėgumų, būtinų, kad galėtų veiksmingai vykdyti savo užduotis, nurodytas 3 dalyje. Valstybės narės užtikrina, kad CSIRT būtų skirta pakankamai išteklių siekiant užtikrinti tinkamą darbuotojų skaičių, kad CSIRT galėtų plėtoti savo techninius pajėgumus.	**KSĮ projektas** **6. Krašto apsaugos ministerija privalo užtikrinti, kad Nacionalinis kibernetinio saugumo centras turėtų pakankamai pajėgumų ir išteklių, reikalingų vykdyti šio straipsnio 2 dalyje nustatytas funkcijas, atitikti šio straipsnio 5 dalyje nustatytus reikalavimus ir plėtoti Nacionalinio kibernetinio saugumo centro techninius pajėgumus.**	Visiškas
3. CSIRT vykdo šias užduotis: a) stebi ir analizuoja kibernetines grėsmes, pažeidžiamumus ir incidentus nacionaliniu lygmeniu, ir, gavusios prašymą, teikia pagalbą atitinkamiems esminiams ir svarbiems subjektams, susijusią su jų tinklų ir informacinių sistemų stebėjimu tikruoju laiku arba beveik tikruoju laiku; b) teikia ankstyvuosius perspėjimus, įspėjimus, pranešimus ir platina informaciją apie kibernetines grėsmes, pažeidžiamumus ir incidentus esminiams ir svarbiems subjektams, taip pat kompetentingoms institucijoms ir kitiems atitinkamiems	**KSĮ projektas** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** **<...>** **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** **1) taiko kibernetinių grėsmių paieškos priemones kibernetinėje erdvėje, siekdamas įvertinti tinklų ir informacinių sistemų atsparumą kibernetiniams incidentams;**	Visiškas

suinteresuotiesiems subjektams, jei įmanoma, beveik tikruoju laiku; c) reaguoja į incidentus ir, kai tikslinga, teikia pagalbą atitinkamiems esminiams ir svarbiems subjektams; d) renka ir analizuoja teismo ekspertizės duomenis ir teikia dinaminę rizikos bei incidentų analizę, taip pat užtikrina informuotumą apie padėtį kibernetinio saugumo srityje; e) esminio ar svarbaus subjekto prašymu aktyviai tikrina atitinkamo subjekto tinklų ir informacines sistemas, kad būtų galima atskleisti pažeidžiamumus, galinčius daryti didelį poveikį; f) dalyvauja CSIRT tinkle ir teikia savitarpio pagalbą pagal savo pajėgumus ir kompetenciją kitiems CSIRT tinklo nariams jų prašymu; g) kai taikytina, atlieka koordinatoriaus funkcijas koordinuoto pažeidžiamumo atskleidimo tikslais pagal 12 straipsnio 1 dalį; h) prisideda prie saugaus dalijimosi informacija priemonių diegimo pagal 10 straipsnio 3 dalį. CSIRT gali atlikti aktyvų neintervencinį esminių ir svarbių subjektų viešai prieinamų tinklų ir informacinių sistemų tikrinimą. Toks tikrinimas atliekamas siekiant aptikti pažeidžiamas arba nesaugiai sukonfigūruotas tinklų ir informacines sistemas ir informuoti atitinkamus subjektus. Toks tikrinimas nedaro jokio neigiamo poveikio subjektų paslaugų veikimui. Vykdydamos pirmoje pastraipoje nurodytas užduotis, CSIRT gali teikti pirmenybę konkrečioms užduotims remdamosi rizika grindžiamu požiūriu.	**2) stebi, renka ir analizuoja informaciją apie kibernetines grėsmes, tinklų ir informacinių sistemų spragas (toliau – spraga), kibernetinius incidentus ir vos neįvykusius kibernetinius incidentus;** **3) valdo kibernetinius incidentus nacionalinio kibernetinių incidentų valdymo plano, tvirtinamo Vyriausybės, nustatyta tvarka;** **4) realiuoju laiku arba beveik realiuoju laiku kibernetinio saugumo subjektams ir suinteresuotiesiems asmenims teikia ankstyvuosius perspėjimus, įspėjimus, pranešimus ir keičiasi informacija apie kibernetines grėsmes, spragas, kibernetinius incidentus ir vos neįvykusius kibernetinius incidentus;** **5) realiuoju laiku arba beveik realiuoju laiku kibernetinio saugumo subjektams teikia pagalbą, susijusią su jų tinklų ir informacinių sistemų stebėjimu;** **6) siekdamas stabdyti kibernetinio incidento poveikį kibernetinio saugumo subjektų tinklų ir informacinių sistemų saugumui, duoda nurodymą viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjams, elektroninių prekyviečių, interneto paieškos sistemų, debesijos kompiuterijos paslaugų teikėjams, elektroninės informacijos prieglobos paslaugų teikėjams ne ilgiau negu 48 valandoms apriboti viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų, elektroninių prekyviečių, interneto paieškos sistemų, debesijos kompiuterijos paslaugų, elektroninės informacijos prieglobos paslaugų teikimą. Nacionalinis kibernetinio saugumo centras apie viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjams pagal šį punktą duotus nurodymus ne vėliau kaip kitą darbo dieną praneša Lietuvos Respublikos ryšių reguliavimo tarnybai;** **7) siekdamas pašalinti kibernetines grėsmes ar stabdyti jų plitimą, duoda nurodymą viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjams, ir (ar) domenų vardų paslaugų teikėjams blokuoti interneto svetainių, platinančių kenkėjiškus kodus, apgaulės būdu renkančius prisijungimus prie tinklų ir informacinių sistemų ir (ar) naudojamus siekiant koordinuoti ir vykdyti kibernetinius incidentus, domenų vardus, taip pat kitus domenų vardus, sukurtus minėtoms interneto svetainių veikloms vykdyti. Nacionalinio kibernetinio saugumo centro sprendimą blokuoti interneto svetainės domeno vardą jos savininkas turi teisę skųsti teismui Lietuvos Respublikos civilinio proceso kodekso nustatyta tvarka;;** **8) kibernetinio incidento metu taiko būtinas kibernetinio saugumo priemones;**	

	9) tikrina kibernetinio saugumo subjektų valdomas ir (ar) tvarkomas tinklų ir informacines sistemas, siekdamas nustatyti spragas; **10) koordinuoja spragų atskleidimą;** **11) renka ir analizuoja kibernetinio incidento tyrimo duomenis ir vykdo kibernetinio saugumo rizikų bei kibernetinių incidentų analizę, taip pat užtikrina kibernetinio saugumo politiką formuojančių ir įgyvendinančių institucijų, taip pat kibernetinio saugumo subjektų informavimą apie padėtį kibernetinio saugumo srityje;** **12) kai būtina informuoti visuomenę siekiant išvengti kibernetinio incidento arba valdyti vykstantį kibernetinį incidentą arba iškilusią kibernetinę grėsmę, prieš tai pasikonsultavęs su kibernetinio saugumo subjektu, pranešusiu apie kibernetinį incidentą, informuoja visuomenę apie kibernetinį incidentą ir (ar) kibernetinę grėsmę, jeigu įmanoma, nurodydamas veiksmus, kurių būtina imtis reaguojant į tą kibernetinį incidentą ir (ar) kibernetinę grėsmę, arba reikalauja, kad tai padarytų informaciją pateikęs kibernetinio saugumo subjektas;** **13) dalyvauja valdant krizes, susijusias su kibernetiniais incidentais, Krizių valdymo ir civilinės saugos įstatymo nustatyta tvarka;** **14) koordinuojant Nacionaliniam krizių valdymo centrui praneša Europos Sąjungos institucijoms apie šio straipsnio 2 dalies 13 punkte nurodytas krizes, kurių viena valstybė narė nepajėgia suvaldyti;** **15) dalyvauja Europos Sąjungos ir NATO įsteigtų reagavimo į kibernetinius incidentus tinklų veikloje ir teikia savitarpio pagalbą pagal savo pajėgumus ir kompetenciją kitiems šių tinklų nariams jų prašymu;**	
4. CSIRT užmezga bendradarbiavimo ryšius su atitinkamais privačiojo sektoriaus suinteresuotaisiais subjektais, kad būtų pasiekti šios direktyvos tikslai.	**KSĮ projektas** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** **<...>** **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** **<...>** **19) kartu su verslo subjektais, mokslo ir studijų institucijomis, nacionalinėmis, Europos Sąjungos, NATO ir kitų valstybių institucijomis ir organizacijomis, tarptautinėmis organizacijomis, nevyriausybinėmis organizacijomis bei kibernetinio saugumo subjektais plėtoja nacionalinį kibernetinį saugumą stiprinančius projektus.**	Visiškas

5. Siekdamos palengvinti bendradarbiavimą, nurodytą 4 dalyje, CSIRT skatina priimti ir naudoti bendrą arba standartizuotą praktiką, klasifikavimo sistemas ir taksonomiją srityse, susijusiose su: a) incidentų valdymo procedūromis; b) krizių valdymu ir c) koordinuotu pažeidžiamumų atskleidimu pagal 12 straipsnio 1 dalį.	**KSĮ projektas** **4 straipsnis. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos** **<...>** **2. Kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos ministerija. Lietuvos Respublikos užsienio reikalų ministerija formuojant kibernetinio saugumo politiką dalyvauja tiek, kiek reikia nustatyti diplomatinių priemonių taikymo reaguojant į kibernetines grėsmes ir kibernetinius incidentus teisinį reguliavimą. Nacionalinis kibernetinio saugumo centras formuojant kibernetinio saugumo politiką dalyvauja tiek, kiek šiame įstatyme nustatytoms funkcijoms atlikti reikia nustatyti kibernetinio saugumo subjektų veiklos ir priežiūros teisinį reguliavimą.** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** **<...>** **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** **<...>** **3) valdo kibernetinius incidentus nacionalinio kibernetinių incidentų valdymo plano, tvirtinamo Vyriausybės, nustatyta tvarka;** **<...>** **10) koordinuoja spragų atskleidimą;** **<...>** **13) dalyvauja valdant krizes, susijusias su kibernetiniais incidentais, Krizių valdymo ir civilinės saugos įstatymo nustatyta tvarka;** **14) koordinuojant Nacionaliniam krizių valdymo centrui praneša Europos Sąjungos institucijoms apie šio straipsnio 2 dalies 13 punkte nurodytas krizes, kurių viena valstybė narė nepajėgia suvaldyti;** **25 straipsnis. Spragų paieška ir atskleidimas** **1. Spragų paieška ir atskleidimas laikomi teisėtais ir tokius veiksmus atlikusiam asmeniui neužtraukia teisinės atsakomybės tik tais atvejais, kai spragų paieška atliekama kibernetinio saugumo subjektų valdomuose ir tvarkomuose tinkluose ir informacinėse sistemose laikantis šio straipsnio 2 dalyje, nacionalinės spragų atskleidimo tvarkos apraše, tvirtinamame krašto**	Visiškas

	apsaugos ministro, ir (ar) kibernetinio saugumo subjekto nustatytos spragų atskleidimo tvarkos apraše, taip pat šio straipsnio 6 dalyje numatytų apribojimų.	
12 straipsnis. Koordinuotas pažeidžiamumų atskleidimas ir Europos pažeidžiamumų duomenų bazė		
1. Kiekviena valstybė narė paskiria vieną iš savo CSIRT koordinuoto pažeidžiamumų atskleidimo koordinatore. Koordinatore paskirta CSIRT veikia kaip patikimas tarpininkas, prireikus lengvinantis sąveiką tarp pranešimą apie pažeidžiamumą teikiančio fizinio ar juridinio asmens ir gamintojo arba potencialiai pažeidžiamų IRT produktų ar IRT paslaugų teikėjo bet kurios šalies prašymu. Koordinatore paskirtos CSIRT užduotys apima: a) atitinkamų subjektų nustatymą ir susisiekimą su jais; b) pagalbos teikimą pranešimus apie pažeidžiamumą teikiantiems fiziniams ar juridiniams asmenims ir c) derybas dėl informacijos atskleidimo terminų ir pažeidžiamumų, kurie daro poveikį keliems subjektams, valdymą. Valstybės narės užtikrina, kad fiziniai ar juridiniai asmenys, jei jie to prašo, galėtų anonimiškai pranešti koordinatore paskirtai CSIRT apie pažeidžiamumą. Koordinatore paskirta CSIRT užtikrina, kad būtų imtasi kruopščių tolesnių veiksmų dėl pažeidžiamumo, apie kurį pranešta, ir užtikrina fizinio ar juridinio asmens, teikiančio pranešimą apie pažeidžiamumą, anonimiškumą. Jeigu pažeidžiamumas, apie kurį pranešta, galėtų daryti didelį poveikį subjektams daugiau nei vienoje valstybėje narėje, kiekvienos susijusios valstybės narės koordinatore paskirta CSIRT, kai tinkama, CSIRT tinkle bendradarbiauja su kitomis koordinatorėmis paskirtomis CSIRT.	**KSĮ projektas** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** **<...>** **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** **<...>** **10) koordinuoja spragų atskleidimą** **25 straipsnis. Spragų paieška ir atskleidimas** **1. Spragų paieška ir atskleidimas laikomi teisėtais ir tokius veiksmus atlikusiam asmeniui neužtraukia teisinės atsakomybės tik tais atvejais, kai spragų paieška atliekama kibernetinio saugumo subjektų valdomuose ir tvarkomuose tinkluose ir informacinėse sistemose laikantis šio straipsnio 2 dalyje, nacionalinės spragų atskleidimo tvarkos apraše, tvirtinamame krašto apsaugos ministro, ir (ar) kibernetinio saugumo subjekto nustatytos spragų atskleidimo tvarkos apraše, taip pat šio straipsnio 6 dalyje numatytų apribojimų.** **2. Atliekant spragų paiešką laikomasi šių apribojimų:** **1) negali būti trikdomas ar keičiamas tinklų ir informacinės sistemos darbas, funkcionalumas, teikiamos paslaugos bei duomenų prieinamumas ar vientisumas;** **2) įsitikinus, kad spraga yra, nutraukiama spragos paieškos veikla, susijusi su aptikta spraga;** **3) subjektas, atlikęs spragų paiešką, ne vėliau kaip per 24 valandas nuo spragų paieškos pradžios (paiešką tęsiant ilgiau kaip 24 valandas – kas 24 valandas) turi parengti nacionalinės spragų atskleidimo tvarkos apraše ar kibernetinio saugumo subjekto nustatytos spragų atskleidimo tvarkos apraše nustatyto turinio informaciją apie spragų paieškos rezultatus ir ją pateikti Nacionaliniam kibernetinio saugumo centrui nacionalinės spragų atskleidimo tvarkos apraše nustatyta tvarka ir (ar) kibernetinio saugumo subjektui, kurio tinklų ir informacinėje sistemoje atlikta spragų paieška, šio kibernetinio saugumo subjekto nustatytos spragų atskleidimo tvarkos apraše nustatyta tvarka;**	Visiškas
2. ENISA, pasikonsultavusi su Bendradarbiavimo grupe, sukuria ir tvarko Europos pažeidžiamumų duomenų bazę. Tuo tikslu ENISA sukuria ir tvarko tinkamas informacines sistemas, politiką ir procedūras ir priima Europos pažeidžiamumų duomenų bazės saugumui ir vientisumui užtikrinti būtinas technines ir organizacines priemones, visų pirma siekdama sudaryti sąlygas		

subjektams, nepriklausomai nuo to, ar jie patenka į šios direktyvos taikymo sritį, bei jų tinklų ir informacinių sistemų tiekėjams, savanoriškai atskleisti ir registruoti viešai žinomas IRT produktų ar IRT paslaugų pažeidžiamumus. Visiems suinteresuotiesiems subjektams suteikiama prieiga prie Europos pažeidžiamumų duomenų bazėje esančios informacijos apie pažeidžiamumus. Toje duomenų bazėje pateikiama: a) informacija, kuria apibūdinamas pažeidžiamumas; b) paveikti IRT produktai ar IRT paslaugos ir pažeidžiamumų rimtumas, atsižvelgiant į aplinkybes, kuriomis juo gali būti pasinaudota; c) informacija apie susijusių pataisų prieinamumą ir, jei pataisų nėra, pažeidžiamų IRT produktų ir IRT paslaugų naudotojams skirtos kompetentingų institucijų arba CSIRT pateiktos gairės, kaip galima sumažinti dėl atskleistų pažeidžiamumų kylančią riziką.	**4) nesiekiama be reikalo, daugiau, negu reikia spragai patvirtinti, stebėti, fiksuoti, perimti, įgyti, laikyti, atskleisti, kopijuoti, keisti, naikinti, gadinti, šalinti, naikinti kibernetinio saugumo subjekto valdomų ir (ar) tvarkomų duomenų;** **5) atskleidžiant spragą nenaudojami pastebėti, užfiksuoti, perimti, atskleisti asmens duomenys;** **6) nebandoma atspėti slaptažodžių, nenaudojami neteisėtu būdu gauti slaptažodžiai ir nėra manipuliuojama kibernetinio saugumo subjekto darbuotojais ar kitais asmenimis, turinčiais teisę naudotis viešai neskelbtina informacija, reikšminga spragų paieškai;** **7) nesidalijama informacija apie aptiktą spragą, išskyrus šios dalies 3 punkte ir šio straipsnio 6 dalyje nustatytus atvejus, taip pat kai informacija apie aptiktą spragą yra registruojama Europos pažeidžiamumų duomenų bazėje.** **3. Subjektas, surinkęs informaciją apie spragą, turi teisę šią informaciją anonimiškai pateikti Nacionaliniam kibernetinio saugumo centrui, išsaugodamas nacionalinės spragų atskleidimo tvarkos apraše nurodytą informaciją apie spragų paieškos rezultatų pateikimą. Nacionalinis kibernetinio saugumo centras užtikrina apie spragą pranešusio subjekto anonimišką. Šioje dalyje nurodytą informaciją apie spragų paieškos rezultatų pateikimą asmuo, surinkęs informaciją apie spragą, ir ją pateikęs anonimiškai, privalo saugoti 12 metų, nuo pranešimo Nacionaliniam kibernetinio saugumo centrui pateikimo dienos.** **4. Spragų atskleidimo Nacionaliniam kibernetinio saugumo centrui tvarka, Nacionaliniam kibernetinio saugumo centrui teikiamos informacijos apie spragas turinys, trumpesnio negu 90 kalendorinių dienų informacijos apie aptiktą spragą atskleidimo kitiems, negu nurodyti šio straipsnio 2 dalies 3 punkte, asmenims termino nustatymo tvarka nustatomi nacionalinės spragų atkleidimo tvarkos apraše.** **5. Kibernetinio saugumo subjektas turi teisę nustatyti spragų jo valdomose ir (ar) tvarkomose tinklų ir informacinėse sistemose atskleidimo tvarką ir nustatyti kitus spragų paieškos apribojimus, negu numatyta šio straipsnio 2 dalyje, arba jų atsisakyti. Kibernetinio saugumo subjekto nustatytame spragų atskleidimo tvarkos apraše numatyti spragų paieškos apribojimai negali būti griežtesni, negu nurodyti šio straipsnio 2 dalyje. Kibernetinio saugumo subjekto nustatytame spragų atskleidimo tvarkos apraše negali būti nustatoma informacijos apie spragas pateikimo Nacionalinio kibernetinio saugumo centro tvarka ir numatomos šio straipsnio 6 dalyje nustatyto reguliavimo išimtys.**	

	6. Subjektas, nustatęs spragą, laikydamasis šio straipsnio 1 dalyje nurodytų apribojimų, turi teisę informaciją apie aptiktą spragą, tačiau ne daugiau, negu buvo pateikta Nacionaliniam kibernetinio saugumo centrui ir (ar) kibernetinio saugumo subjektui, atskleisti kitiems, negu nurodyti šio straipsnio 2 dalies 3 punkte, asmenims ne anksčiau kaip po 90 kalendorinių dienų nuo informacijos apie spragą pateikimo Nacionaliniam kibernetinio saugumo centrui ir (ar) kibernetinio saugumo subjektui. Nacionalinis kibernetinio saugumo centras, įvertinęs spragos sudėtingumą ir jos ištaisymo galimybes, nacionalinės spragų atskleidimo tvarkos apraše nustatyta tvarka turi teisę nustatyti trumpesnį informacijos apie aptiktą spragą atskleidimo kitiems, negu nurodyti šio straipsnio 2 dalies 3 punkte, asmenims terminą, tačiau ne trumpesnį kaip 3 kalendorinės dienos.	
13 straipsnis. Bendradarbiavimas nacionaliniu lygmeniu		
1. Kai tos pačios valstybės narės kompetentingos institucijos, bendrasis kontaktinis punktas ir CSIRT yra atskiri, jie bendradarbiauja tarpusavyje, kad vykdytų šioje direktyvoje nustatytas pareigas.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes KSĮ projekto 7 straipsnio 2 dalyje nustatyta, kad Nacionalinis kibernetinio saugumo centras vykdo visas Direktyvos nuostatoje išvardintas funkcijas*.	
2. Valstybės narės užtikrina, kad jų CSIRT arba, kai taikytina, kompetentingos institucijos gautų pranešimus apie didelius incidentus pagal 23 straipsnį ir incidentus, dideles kibernetines grėsmes ir vos neįvykusius incidentus pagal 30 straipsnį.	**KSĮ projektas** **18 straipsnis. Pranešimai apie kibernetinius incidentus** **1. Kibernetinio saugumo subjektai privalo pranešti Nacionaliniam kibernetinio saugumo centrui apie:** **1) didelį kibernetinį incidentą, darantį poveikį jų šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus atitinkančiai vykdomai veiklai ir (ar) teikiamoms paslaugoms;** **2) šios dalies 1 punkte nenurodytus kibernetinius incidentus, darančius poveikį jų šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus atitinkančiai vykdomai veiklai ir (ar) teikiamoms paslaugoms nacionalinio kibernetinių incidentų valdymo plano, tvirtinamo Vyriausybės, nustatytais terminais ir pateikiant Vyriausybės nustatytą informaciją.** **<...>** **5. Kibernetinio saugumo subjektai privalo pranešti apie kibernetinį incidentą ir kibernetinę grėsmę nacionalinio kibernetinių incidentų valdymo plano, tvirtinamo Vyriausybės, nustatyta tvarka.**	Visiškas

3. Valstybės narės užtikrina, kad jų CSIRT arba, kai taikytina, kompetentingos institucijos informuotų savo bendruosius kontaktinius punktus apie šioje direktyvoje nustatyta tvarka pateikiamus pranešimus apie incidentus, kibernetines grėsmes ir vos neįvykusius incidentus.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes KSĮ projekto 7 straipsnio 2 dalyje nustatyta, kad Nacionalinis kibernetinio saugumo centras vykdo visas Direktyvos nuostatoje išvardintas funkcijas.*	
4. Siekiant užtikrinti, kad kompetentingų institucijų, bendrųjų kontaktinių punktų ir CSIRT užduotys ir pareigos būtų vykdomos veiksmingai, valstybės narės užtikrina tinkamą tų įstaigų ir teisėsaugos institucijų, duomenų apsaugos institucijų, nacionalinių institucijų pagal reglamentus (EB) Nr. 300/2008 ir (ES) 2018/1139, priežiūros įstaigų pagal Reglamentą (ES) Nr. 910/2014, kompetentingų institucijų pagal Reglamentą (ES) 2022/2554, nacionalinių reguliavimo institucijų pagal Direktyvą (ES) 2018/1972, kompetentingų institucijų pagal Direktyvą (ES) 2022/2557, taip pat kompetentingų institucijų pagal kitus konkretiems sektoriams taikomus Sąjungos teisės aktus bendradarbiavimą toje valstybėje narėje.	**KSĮ projektas** **20 straipsnis. Tarpinstitucinis bendradarbiavimas** **1. Kibernetinio saugumo politiką formuojančios ir įgyvendinančios institucijos bendradarbiauja tarpusavyje bei su kitomis valstybės institucijomis įgyvendindamos šiame įstatyme nustatytus tikslus, įskaitant keitimąsi informacija ir duomenimis apie kibernetinius incidentus, kibernetines grėsmes ir vos neįvykusius kibernetinius incidentus, taip pat informacijos perdavimą pagal šio straipsnio 2 dalį.** **2. Nacionalinis kibernetinio saugumo centras:** **1) ne vėliau kaip per 20 darbo dienų nuo sprendimo taikyti šio įstatymo 28 straipsnio 1 dalyje nurodytą vykdymo užtikrinimo priemonę priėmimo apie tai informuoja kompetentingą instituciją pagal Krizių valdymo ir civilinės saugos įstatymą, jeigu vykdymo užtikrinimo priemonė taikoma siekiant užtikrinti, kad esminis subjektas laikytųsi šio įstatymo reikalavimų;** **2) ne vėliau kaip per 20 darbo dienų nuo sprendimo taikyti šio įstatymo 28 straipsnio 1 dalyje vykdymo užtikrinimo priemonę priėmimo apie tai informuoja kompetentingą instituciją pagal Reglamentą (ES) 2022/2554, jeigu vykdymo užtikrinimo priemonė taikoma siekiant užtikrinti, kad esminis subjektas, kuris paskirtas ypatingai svarbiu trečiųjų šalių informacinių ir ryšių technologijų paslaugų teikėju pagal Reglamento (ES) 2022/2554 31 straipsnį, laikytųsi šio įstatymo reikalavimų;** **3) turi teisę su kompetentinga institucija pagal Reglamentą (ES) 2022/2554 sudaryti bendradarbiavimo susitarimą, nurodytą Reglamento (ES) 2022/2554 47 straipsnio 3 dalyje;** **4) nustatęs, kad esminis ar svarbus subjektas gali būti padaręs asmens duomenų saugumo pažeidimą, apie tai nepagrįstai nedelsiant, bet ne vėliau kaip per 72 valandas nuo šios aplinkybės nustatymo, informuoja Valstybinę duomenų apsaugos inspekciją nurodydamas turimą informaciją apie Reglamento (ES) 2016/679 33 straipsnio 3 dalyje nurodytas aplinkybes;** **5) bendradarbiauja su Lietuvos Respublikos ryšių reguliavimo tarnyba dėl patikimumo užtikrinimo paslaugų teikėjų kibernetinio saugumo audito**	Visiškas
5. Valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą ir jų kompetentingos institucijos pagal Direktyvą (ES) 2022/2557 bendradarbiautų ir reguliariai keistųsi informacija, kiek tai susiję su ypatingos svarbos subjektų identifikavimu, apie riziką, kibernetines grėsmes, ir incidentus, taip pat apie nekibernetinę riziką, grėsmes ir incidentus, darančius poveikį subjektams, kurie pagal Direktyvą (ES) 2022/2557 identifikuoti kaip ypatingos svarbos subjektai, ir apie priemones, kurių imtasi reaguojant į tą riziką, grėsmes ir incidentus. Valstybės narės taip pat užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą ir jų kompetentingos institucijos pagal Reglamentą (ES) Nr. 910/2014, Reglamentą (ES) 2022/2554 ir Direktyvą (ES) 2018/1972 reguliariai keistųsi atitinkama informacija, be kita ko, susijusia su atitinkamais incidentais ir kibernetinėmis grėsmėmis.		Visiškas

	srityje, ir nedelsiant, be ne vėliau kaip per 24 val. informuoja Lietuvos Respublikos ryšių reguliavimo tarnybą apie patikimumo užtikrinimo paslaugų teikėjų praneštus kibernetinius incidentus; **6) ne vėliau kaip per 20 darbo dienų nuo sprendimo taikyti šio įstatymo 28 straipsnio 1 dalyje vykdymo užtikrinimo priemonę priėmimo apie tai informuoja kitos valstybės narės kompetentingą instituciją, atsakingą už kibernetinio saugumo reikalavimų vykdymo užtikrinimą, jeigu kibernetinio saugumo subjektas teikia paslaugas arba jo tinklų ir informacinės sistemos yra toje valstybėje narėje;** **7) bendradarbiauja su kitų valstybių narių kompetentingomis institucijos, atsakingomis už kibernetinio saugumo reikalavimų vykdymo užtikrinimą, kai kibernetinio saugumo subjektas teikia paslaugas daugiau nei vienoje valstybėje narėje arba teikia paslaugas vienoje ar daugiau valstybių narių, o jo tinklų ir informacinės sistemos yra vienoje ar daugiau kitų valstybių narių, vykdydamos savitarpio pagalbos prašymus šios įstatymo 21 straipsnio nustatyta tvarka.**	
6. Valstybės narės techninėmis priemonėmis supaprastina informacijos, susijusios su 23 ir 30 straipsniuose nurodytais pranešimais, teikimą.	**KSĮ projektas** **19 straipsnis. Kibernetinio saugumo informacinis tinklas** **1. Kibernetinio saugumo informacinis tinklas yra valstybės informacinė sistema, kurios paskirtis:** <...> **5) keistis su Kibernetinio saugumo informacinio tinklo naudotojais duomenimis, susijusiais su kibernetiniais incidentais, kibernetinėmis grėsmėmis, vos neįvykusiais kibernetiniais incidentais, taip pat kita su kibernetinio saugumo užtikrinimu susijusia informacija.**	Visiškas
14 straipsnis. Bendradarbiavimo grupė		
1. Siekiant remti ir palengvinti strateginį bendradarbiavimą ir keitimąsi informacija tarp valstybių narių, taip pat sustiprinti pasitikėjimą ir patikimumą, sudaroma Bendradarbiavimo grupė.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
2. Bendradarbiavimo grupė vykdo savo užduotis remdamasi dvimetėmis darbo programomis, nurodytomis 7 dalyje.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
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	**KSĮ projektas** **5 straipsnis. Krašto apsaugos ministerijos įgaliojimai kibernetinio saugumo srityje**	Visiškas

institucijos pagal Reglamentą (ES) 2022/2554 gali dalyvauti Bendradarbiavimo grupės veikloje pagal to reglamento 47 straipsnio 1 dalį. Prireikus Bendradarbiavimo grupė gali pakviesti Europos Parlamentą ir atitinkamų suinteresuotųjų subjektų atstovus dalyvauti jos darbe. Komisija teikia sekretoriato paslaugas.	**Krašto apsaugos ministerija, be šio įstatymo 4 straipsnio 2 dalyje numatyto kibernetinio saugumo politikos formavimo ir kitų šio įstatymo nustatytų funkcijų vykdymo, taip pat bendradarbiauja su atitinkamomis Šiaurės Atlanto sutarties organizacijos (toliau – NATO) bei Europos Sąjungos ir NATO bei Europos Sąjungos valstybių institucijomis, tarptautinėmis institucijomis kibernetinio saugumo klausimais.**	
4. Bendradarbiavimo grupė vykdo šias užduotis: a) teikia kompetentingoms institucijoms gaires dėl šios direktyvos perkėlimo į nacionalinę teisę ir įgyvendinimo; b) teikia kompetentingoms institucijoms gaires, susijusias su koordinuoto pažeidžiamumų atskleidimo politikos plėtojimu ir įgyvendinimu, kaip nurodyta 7 straipsnio 2 dalies c punkte; c) keičiasi geriausios praktikos pavyzdžiais ir informacija, susijusia su šios direktyvos įgyvendinimu, įskaitant informaciją, susijusią su kibernetinėmis grėsmėmis, incidentais, pažeidžiamumais, vos neįvykusiais incidentais, informuotumo didinimo iniciatyvomis, mokymu, pratybomis ir įgūdžiais, gebėjimų stiprinimu, standartais ir techninėmis specifikacijomis, taip pat su esminių ir svarbių subjektų identifikavimu pagal 2 straipsnio 2 dalies b–e punktus; d) keičiasi patarimais ir bendradarbiauja su Komisija dėl naujų kibernetinio saugumo politikos iniciatyvų ir bendro konkretiems sektoriams taikomų kibernetinio saugumo reikalavimų nuoseklumo; e) keičiasi patarimais ir bendradarbiauja su Komisija dėl deleguotųjų arba įgyvendinimo aktų, priimamų pagal šią direktyvą, projektų; f) keičiasi geriausios praktikos pavyzdžiais ir informacija su atitinkamomis Sąjungos institucijomis, įstaigomis, organais ir agentūromis; g) keičiasi nuomonėmis dėl konkretiems sektoriams taikomų Sąjungos teisės aktų, kuriuose yra nuostatų dėl kibernetinio saugumo, įgyvendinimo; h) kai tinkama, aptaria 19 straipsnio 9 dalyje nurodytas tarpusavio vertinimo ataskaitas ir parengia išvadas ir rekomendacijas;	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	

i) atlieka koordinuojamus ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimus pagal 22 straipsnio 1 dalį; j) aptaria savitarpio pagalbos atvejus, įskaitant patirtį ir rezultatus, susijusius su bendrais tarpvalstybiniais priežiūros veiksmais, kaip nurodyta 37 straipsnyje; k) vienos ar daugiau atitinkamų valstybių narių prašymu aptaria konkrečius savitarpio pagalbos prašymus, nurodytus 37 straipsnyje; l) teikia strategines gaires CSIRT tinklui ir EU–CyCLONe konkrečiais kylančiais klausimais; m) keičiasi nuomonėmis dėl politikos dėl tolesnių veiksmų po didelio masto kibernetinio saugumo incidentų ir krizių remiantis CSIRT tinklo ir EU-CyCLONe patirtimi; n) prisideda prie kibernetinio saugumo pajėgumų visoje Sąjungoje palengvindama nacionalinių pareigūnų mainus pagal gebėjimų stiprinimo programą, kurioje dalyvauja kompetentingų institucijų arba CSIRT darbuotojai; o) organizuoja nuolatinius bendrus susitikimus su atitinkamais privačiais suinteresuotaisiais subjektais iš visos Sąjungos, kad aptartų Bendradarbiavimo grupės vykdomą veiklą ir surinktų informacijos apie naujus politikos uždavinius; p) aptaria su kibernetinio saugumo pratybomis susijusį darbą, įskaitant ENISA atliktą darbą; q) nustato 19 straipsnio 1 dalyje nurodytų tarpusavio vertinimų metodiką ir organizacinius aspektus, taip pat, padedant Komisijai ir ENISA, pagal 19 straipsnio 5 dalį nustato valstybėms narėms savęs vertinimo metodiką, ir, bendradarbiaudama su Komisija ir ENISA, parengia elgesio kodeksus, kuriais grindžiami pagal 19 straipsnio 6 dalį paskirtų kibernetinio saugumo ekspertų darbo metodai; r) 40 straipsnyje nurodytos peržiūros tikslais rengia Komisijai strateginiu lygmeniu ir atliekant tarpusavio vertinimus sukauptos patirties ataskaitas; s) aptaria ir reguliariai vertina kibernetinių grėsmių ar incidentų, pavyzdžiui, susijusių su išpirkos reikalavimo programine įranga, padėtį.		

Bendradarbiavimo grupė teikia pirmos pastraipos r punkte nurodytas ataskaitas Komisijai, Europos Parlamentui ir Tarybai.		
5. Valstybės narės užtikrina efektyvų, veiksmingą ir saugų savo atstovų Bendradarbiavimo grupėje bendradarbiavimą.		
6. Bendradarbiavimo grupė gali prašyti, kad CSIRT tinklas parengtų techninę ataskaitą pasirinktomis temomis.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
7. Ne vėliau kaip 2024 m. vasario 1 d., o vėliau – kas dvejus metus Bendradarbiavimo grupė parengia darbo programą, skirtą veiksmams, kurių reikia imtis jos tikslams ir užduotims įgyvendinti.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
8. Komisija gali priimti įgyvendinimo aktus, kuriais nustatoma procedūrinė tvarka, būtina Bendradarbiavimo grupės veikimui užtikrinti. Tie įgyvendinimo aktai priimami laikantis 39 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros. Komisija keičiasi rekomendacijomis ir bendradarbiauja su Bendradarbiavimo grupe dėl šios dalies pirmoje pastraipoje nurodytų įgyvendinimo aktų projektų pagal 4 dalies e punktą.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
9. Bendradarbiavimo grupė nuolat ir ne rečiau kaip kartą per metus susitinka su Ypatingos svarbos subjektų atsparumo klausimų grupe, sudaryta pagal Direktyvą (ES) 2022/2557, kad skatintų ir palengvintų strateginį bendradarbiavimą ir keitimąsi informacija.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
15 straipsnis. CSIRT tinklas		
1. Siekiant prisidėti prie pasitikėjimo ir atsakomybės didinimo, taip pat skatinti greitą ir veiksmingą valstybių narių operatyvinį bendradarbiavimą, sukuriamas nacionalinių CSIRT tinklas.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
2. CSIRT tinklą sudaro pagal 10 straipsnį paskirtų arba įsteigtų CSIRT ir Sąjungos institucijų, įstaigų ir agentūrų kompiuterinių incidentų tyrimo tarnybos (CERT-EU) atstovai. Komisija dalyvauja CSIRT tinklo veikloje stebėtojos teisėmis. ENISA teikia sekretoriato paslaugas ir aktyviai teikia pagalbą CSIRT tarpusavio bendradarbiavimo srityje.	**KSĮ projektas** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** **<...>** **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** **<...>**	Visiškas

	15) dalyvauja Europos Sąjungos ir NATO įsteigtų reagavimo į kibernetinius incidentus tinklų veikloje ir teikia savitarpio pagalbą pagal savo pajėgumus ir kompetenciją kitiems šių tinklų nariams jų prašymu.	
3. CSIRT tinklas vykdo šias užduotis: a) keičiasi informacija apie CSIRT pajėgumus; b) padeda CSIRT tarpusavyje dalytis technologijomis ir atitinkamomis priemonėmis, politika, įrankiais, procesais, geriausios praktikos pavyzdžiais ir sistemomis ir juos perduoti bei jais keistis; c) keičiasi svarbia informacija apie incidentus, vos neįvykusius incidentus, kibernetines grėsmes, riziką ir pažeidžiamumus; d) keičiasi informacija apie kibernetinio saugumo leidinius ir rekomendacijas; e) užtikrina sąveikumą, susijusį su dalijimosi informacija specifikacijomis ir protokolais; f) CSIRT tinklo, kuris galėjo būti paveiktas incidento, nario prašymu keičiasi informacija, susijusia su tuo incidentu ir atitinkamomis kibernetinėmis grėsmėmis, rizika ir pažeidžiamumais, ir ją aptaria; g) CSIRT tinklo nario prašymu aptaria ir, kai įmanoma, įgyvendina koordinuotą atsaką į incidentą, nustatytą tos valstybės narės jurisdikcijoje; h) teikia valstybėms narėms pagalbą šalinant tarpvalstybinius incidentus pagal šią direktyvą; i) bendradarbiauja, keičiasi geriausios praktikos pavyzdžiais ir teikia pagalbą pagal 12 straipsnio 1 dalį koordinatorėmis paskirtoms CSIRT, kiek tai susiję su koordinuoto pažeidžiamumų, galinčių daryti didelį poveikį subjektams daugiau nei vienoje valstybėje narėje, atskleidimo valdymu; j) aptaria ir nustato tolesnes operatyvinio bendradarbiavimo formas, be kita ko, susijusias su: i) kibernetinių grėsmių ir incidentų kategorijomis; ii) ankstyvaisiais perspėjimais; iii) savitarpio pagalba; iv) koordinavimo principais ir tvarka reaguojant į tarpvalstybinę riziką ir incidentus;	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	

v) pagalba rengiant nacionalinį reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planą, nurodytą 9 straipsnio 4 dalyje, teikiama valstybės narės prašymu; k) informuoja Bendradarbiavimo grupę apie savo veiklą ir tolesnes operatyvinio bendradarbiavimo formas, aptartas pagal j punktą, ir prireikus prašo tuo klausimu pateikti rekomendacijų; l) įvertina kibernetinio saugumo pratybas, įskaitant ENISA organizuojamas pratybas; m) atskiros CSIRT prašymu aptaria tos CSIRT pajėgumus ir parengtį; n) bendradarbiauja ir keičiasi informacija su regioniniais ir Sąjungos lygmens saugumo operacijų centrais (SOC), kad pagerintų bendrą informuotumą apie padėtį, susijusią su incidentais ir grėsmėmis visoje Sąjungoje; o) kai tinkama, aptaria 19 straipsnio 9 dalyje nurodytas tarpusavio vertinimo ataskaitas; p) teikia gaires siekiant palengvinti operatyvinės praktikos konvergenciją taikant šio straipsnio nuostatas dėl operatyvinio bendradarbiavimo.		
4. Ne vėliau kaip 2025 m. sausio 17 d., o vėliau – kas dvejus metus CSIRT tinklas 40 straipsnyje nurodytos priežiūros tikslais įvertina padarytą pažangą operatyvinio bendradarbiavimo srityje ir patvirtina ataskaitą. Ataskaitoje visų pirma pateikiamos išvados ir rekomendacijos, grindžiamos 19 straipsnyje nurodytų tarpusavio vertinimų, atliktų dėl nacionalinių CSIRT, rezultatais. Ta ataskaita pateikiama Bendradarbiavimo grupei.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
5. CSIRT tinklas priima savo darbo tvarkos taisykles.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
6. CSIRT tinklas ir EU-CyCLONe susitaria dėl procedūrinės tvarkos ir ja remdamiesi bendradarbiauja.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
16 straipsnis. Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas (EU-CyCLONe)		
1. Siekiant remti koordinuotą didelio masto kibernetinio saugumo incidentų ir krizių valdymą operatyviniu lygmeniu ir užtikrinti reguliarų keitimąsi svarbia informacija tarp valstybių narių ir	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	

Sąjungos institucijų, įstaigų, organų ir agentūrų, įsteigiamas EU-CyCLONe.		
2. EU-CyCLONe sudaro valstybių narių kibernetinių krizių valdymo institucijų atstovai, taip pat tais atvejais, kai galimas arba vykstantis didelio masto kibernetinio saugumo incidentas turi arba gali turėti didelį poveikį paslaugoms ir veiklai, kurioms taikoma ši direktyva – Komisijos atstovai. Kitais atvejais Komisija dalyvauja EU-CyCLONe veikloje stebėtojo teisėmis. ENISA teikia EU-CyCLONe sekretoriato paslaugas ir padeda saugiai keistis informacija, taip pat teikia būtinas priemones valstybių narių tarpusavio bendradarbiavimui remti, užtikrinančias saugų keitimąsi informacija. Kai tikslinga, EU-CyCLONe gali pakviesti atitinkamų suinteresuotųjų subjektų atstovus dalyvauti jo darbe stebėtojų teisėmis.	**KSĮ projektas** **5 straipsnis. Krašto apsaugos ministerijos įgaliojimai kibernetinio saugumo srityje** **Krašto apsaugos ministerija, be šio įstatymo 4 straipsnio 2 dalyje numatyto kibernetinio saugumo politikos formavimo ir kitų šio įstatymo nustatytų funkcijų vykdymo, taip pat bendradarbiauja su atitinkamomis Šiaurės Atlanto sutarties organizacijos (toliau – NATO) bei Europos Sąjungos ir NATO bei Europos Sąjungos valstybių institucijomis, tarptautinėmis institucijomis kibernetinio saugumo klausimais.** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** **<...>** **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** **<...>** **13) dalyvauja valdant krizes, susijusias su kibernetiniais incidentais, Krizių valdymo ir civilinės saugos įstatymo nustatyta tvarka;** **14) koordinuojant Nacionaliniam krizių valdymo centrui praneša Europos Sąjungos institucijoms apie šio straipsnio 2 dalies 13 punkte nurodytas krizes, kurių viena valstybė narė nepajėgia suvaldyti;** **15) dalyvauja Europos Sąjungos ir NATO įsteigtų reagavimo į kibernetinius incidentus tinklų veikloje ir teikia savitarpio pagalbą pagal savo pajėgumus ir kompetenciją kitiems šių tinklų nariams jų prašymu.**	Visiškas
3. EU-CyCLONe vykdo šias užduotis: a) didina pasirengimo valdyti didelio masto kibernetinio saugumo incidentus ir krizes lygį; b) plėtoja bendrą informuotumą apie padėtį, susijusią su didelio masto kibernetinio saugumo incidentais ir krizėmis; c) įvertina atitinkamų didelio masto kibernetinio saugumo incidentų pasekmes ir poveikį ir siūlo galimas švelninimo priemones; d) koordinuoja didelio masto kibernetinio saugumo incidentų ir krizių valdymą ir padeda politiniu lygmeniu priimti sprendimus, susijusius su tokiais incidentais ir krizėmis;	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	

e) atitinkamos valstybės narės prašymu aptaria 9 straipsnio 4 dalyje nurodytus nacionalinius reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planus.		
4. EU-CyCLONe priima savo darbo tvarkos taisykles.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
5. EU-CyCLONe reguliariai teikia ataskaitas Bendradarbiavimo grupei apie didelio masto kibernetinio saugumo incidentų ir krizių valdymą, taip pat apie tendencijas, ypatingą dėmesį skirdamas jų poveikiui esminiams ir svarbiems subjektams.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
6. EU-CyCLONe su CSIRT tinklu bendradarbiauja remdamasis sutartomis procedūrinėmis taisyklėmis, numatytomis 15 straipsnio 6 dalyje.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
7. Ne vėliau kaip 2024 m. liepos 17 d., o vėliau – kas 18 mėnesių EU-CyCLONe teikia Europos Parlamentui ir Tarybai savo darbo įvertinimo ataskaitą.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
17 straipsnis. Tarptautinis bendradarbiavimas Pagal SESV 218 straipsnį Sąjunga, kai tinkama, gali sudaryti tarptautinius susitarimus su trečiosiomis valstybėmis ar tarptautinėmis organizacijomis, pagal kuriuos joms būtų leidžiama dalyvauti tam tikroje Bendradarbiavimo grupės, CSIRT tinklo ir EU-CyCLONe veikloje ir toks dalyvavimas būtų organizuojamas. Tokie susitarimai turi atitikti Sąjungos duomenų apsaugos teisės aktus.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
18 straipsnis. Kibernetinio saugumo būklės Sąjungoje ataskaita		
1. ENISA, bendradarbiaudama su Komisija ir Bendradarbiavimo grupe, kas dvejus metus patvirtina kibernetinio saugumo Sąjungoje būklės ataskaitą ir tą ataskaitą pateikia ir pristato Europos Parlamentui. Ataskaita, inter alia, paskelbiama kaip kompiuterio skaitomi duomenys ir į ją turi būti įtraukti šie aspektai: a) Sąjungos lygmens kibernetinio saugumo rizikos vertinimas, kuriame atsižvelgiama į kibernetinių grėsmių padėtį; b) kibernetinio saugumo pajėgumų plėtojimo viešajame ir privačiajame sektoriuose visoje Sąjungoje vertinimas;	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	

c) piliečių ir subjektų, įskaitant mažąsias ir vidutines įmones, bendro informuotumo apie kibernetinį saugumą ir kibernetinės higienos lygio vertinimas; d) 19 straipsnyje nurodytų tarpusavio vertinimų rezultatų apibendrintas vertinimas; e) apibendrintas kibernetinio saugumo pajėgumų ir išteklių brandos lygio visoje Sąjungoje, be kita ko, sektorių lygmeniu, taip pat valstybių narių nacionalinių kibernetinio saugumo strategijų suderinimo masto vertinimas.		
2. Ataskaitoje pateikiamos konkrečios politikos rekomendacijos, kaip pašalinti trūkumus ir padidinti kibernetinio saugumo lygį visoje Sąjungoje, ir konkretaus laikotarpio išvadų santrauka iš agentūros ES kibernetinio saugumo techninės padėties ataskaitų dėl incidentų ir kibernetinių grėsmių, kurias pagal Reglamento (ES) 2019/881 7 straipsnio 6 dalį parengė ENISA.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
3. ENISA, bendradarbiaudama su Komisija, Bendradarbiavimo grupe ir CSIRT tinklu, parengia metodiką, į kurią būtų įtraukiami atitinkami 1 dalies e punkte nurodyto apibendrinto vertinimo kintamieji, pavyzdžiui, kiekybiniai ir kokybiniai rodikliai.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
19 straipsnis. Tarpusavio vertinimai		
1. Bendradarbiavimo grupė, padedant Komisijai ir ENISA bei, kai tinkama, CSIRT, ne vėliau kaip 2025 m. sausio 17 d. nustato tarpusavio vertinimų metodiką ir organizacinius aspektus, kad būtų galima pasimokyti iš bendros patirties, stiprinti tarpusavio pasitikėjimą, pasiekti aukštą bendrą kibernetinio saugumo lygį, taip pat stiprinti valstybių narių kibernetinio saugumo pajėgumus ir politiką, būtinus šiai direktyvai įgyvendinti. Dalyvavimas tarpusavio vertinimuose yra savanoriškas. Tarpusavio vertinimus atlieka kibernetinio saugumo ekspertai. Kibernetinio saugumo ekspertus skiria bent dvi valstybės narės, kurios nėra vertinamosios valstybės narės. Tarpusavio vertinimai apima bent vieną iš šių aspektų: a) kibernetinio saugumo rizikos valdymo priemonių ir pareigų pranešti, įtvirtintų 21 ir 23 straipsniuose, įgyvendinimo lygį;	**KSĮ projektas** **5 straipsnis. Krašto apsaugos ministerijos įgaliojimai kibernetinio saugumo srityje** **Krašto apsaugos ministerija, be šio įstatymo 4 straipsnio 2 dalyje numatyto kibernetinio saugumo politikos formavimo ir kitų šio įstatymo nustatytų funkcijų vykdymo, taip pat bendradarbiauja su atitinkamomis Šiaurės Atlanto sutarties organizacijos (toliau – NATO) bei Europos Sąjungos ir NATO bei Europos Sąjungos valstybių institucijomis, tarptautinėmis institucijomis kibernetinio saugumo klausimais.** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** <...> **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** <...>	Visiškas

b) gebėjimų lygį, įskaitant turimus finansinius, techninius ir žmogiškuosius išteklius, ir kompetentingų institucijų užduočių vykdymo veiksmingumą; c) CSIRT operatyvinius pajėgumus; d) 37 straipsnyje nurodytos savitarpio pagalbos įgyvendinimo lygį; e) 29 straipsnyje nurodytų keitimosi kibernetinio saugumo informacija susitarimų įgyvendinimo lygį; f) konkrečius tarpvalstybinio arba tarpsektorinio pobūdžio klausimus.	**18) bendradarbiauja su Europos Sąjungos, NATO ir kitų valstybių institucijomis ir organizacijomis, įgyvendinančiomis kibernetinio saugumo politiką, tarptautinėmis organizacijomis, turi teisę jas pasitelkti kartu atliekant šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje;** **19) kartu su verslo subjektais, mokslo ir studijų institucijomis, nacionalinėmis, Europos Sąjungos, NATO ir kitų valstybių institucijomis ir organizacijomis, tarptautinėmis organizacijomis, nevyriausybinėmis organizacijomis bei kibernetinio saugumo subjektais plėtoja nacionalinį kibernetinį saugumą stiprinančius projektus.**	
2. 1 dalyje nurodyta metodika apima objektyvius, nediskriminacinius, sąžiningus ir skaidrius kriterijus, kuriais remdamosi valstybės narės paskiria kibernetinio saugumo ekspertus, atitinkančius reikalavimus tarpusavio vertinimui atlikti. Komisija ir ENISA dalyvauja tarpusavio vertinimuose stebėtojų teisėmis.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
3. Valstybės narės gali nustatyti konkrečius 1 dalies f punkte nurodytus klausimus tarpusavio vertinimui.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
4. Prieš pradėdamos 1 dalyje nurodytą tarpusavio vertinimą, valstybės narės praneša dalyvaujančioms valstybėms narėms jo apimtį, įskaitant konkrečius klausimus, nustatytus pagal 3 dalį.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
5. Prieš pradėdamos tarpusavio vertinimą, valstybės narės gali pačios įvertinti vertinamus aspektus ir pateikti tą įsivertinimą paskirtiems kibernetinio saugumo ekspertams. Bendradarbiavimo grupė, padedant Komisijai ir ENISA, nustato valstybių narių įsivertinimo metodiką.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
6. Tarpusavio vertinimai apima fizinius arba virtualius apsilankymus vietoje ir keitimąsi informacija ne vietoje. Laikantis gero bendradarbiavimo principo, valstybės narės, kurioms taikomas tarpusavio vertinimas, pateikia paskirtiems kibernetinio saugumo ekspertams vertinimui atlikti reikalingą informaciją; tai daroma nedarant poveikio Sąjungos ar nacionalinei teisei dėl konfidencialios ar įslaptintos informacijos apsaugos ir esminių valstybės funkcijų, pavyzdžiui, nacionalinio saugumo, apsaugai. Bendradarbiavimo grupė,	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	

bendradarbiaudama su Komisija ir ENISA, parengia atitinkamus elgesio kodeksus, kuriais grindžiami paskirtų kibernetinio saugumo ekspertų darbo metodai. Visa per tarpusavio vertinimą gauta informacija naudojama tik tam vertinimui. Tarpusavio vertinime dalyvaujantys kibernetinio saugumo ekspertai neatskleidžia jokios per tą tarpusavio vertinimą gautos neskelbtinos ar konfidencialios informacijos jokioms trečiosioms šalims.		
7. Atlikus tarpusavio vertinimą, tų pačių valstybėje narėje peržiūrėtų aspektų tolesnis tarpusavio vertinimas toje valstybėje narėje dvejus metus po tarpusavio vertinimo pabaigos neatliekamas, nebent valstybė narė prašytų arba Bendradarbiavimo grupei pasiūlius būtų susitarta kitaip.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
8. Valstybės narės užtikrina, kad bet kokia su paskirtais kibernetinio saugumo ekspertais susijusi interesų konflikto rizika būtų atskleista kitoms valstybėms narėms, Bendradarbiavimo grupei, Komisijai ir ENISA prieš pradedant tarpusavio vertinimą. Valstybė narė, kuriai taikomas tarpusavio vertinimas, gali dėl tinkamai pagrįstų priežasčių, apie kurias pranešta paskiriančiai valstybei narei, paprieštarauti tam, kad būtų paskirti konkretūs kibernetinio saugumo ekspertai.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
9. Tarpusavio vertinimuose dalyvaujantys kibernetinio saugumo ekspertai parengia per tarpusavio vertinimus nustatytų faktų ir išvadų ataskaitas. Valstybės narės, kurioms taikomas tarpusavio vertinimas, gali teikti pastabas dėl su jomis susijusių ataskaitų projektų ir tokios pastabos pridedamos prie ataskaitų. Ataskaitose pateikiamos rekomendacijos, kaip pagerinti aspektus, kuriuos apėmė tarpusavio vertinimas. Kai tinkama, ataskaitos pateikiamos Bendradarbiavimo grupei ir CSIRT tinklui. Valstybė narė, kuriai taikomas tarpusavio vertinimas, gali nuspręsti savo ataskaitą arba jos redaguotą versiją padaryti viešai prieinamą.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
20 straipsnis. Valdymas		
1. Valstybės narės užtikrina, kad esminių ir svarbių subjektų valdymo organai patvirtintų kibernetinio saugumo rizikos valdymo priemones, kurių ėmėsi tie subjektai, siekdami laikytis	**KSĮ projektas** **14 straipsnis. Kibernetinio saugumo rizikos valdymo priemonės**	Visiškas

21 straipsnio, prižiūrėtų jo įgyvendinimą ir galėtų būti patraukti atsakomybėn už tai, kad subjektai pažeidžia tą straipsnį. Šios dalies taikymu nedaromas poveikis nacionalinės teisės aktams, susijusiems su atsakomybės taisyklėmis, taikomomis viešosioms institucijoms, taip pat valstybės tarnautojų ir renkamų ar paskirtų pareigūnų atsakomybe.	**1. Kibernetinio saugumo subjektai privalo užtikrinti šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus atitinkančiai veiklai vykdyti ar paslaugoms teikti naudojamų tinklų ir informacinių sistemų atitiktį kibernetinio saugumo rizikos valdymo priemonėms:** **1) kibernetinio saugumo reikalavimams, tvirtinamiems Vyriausybės, išskyrus šio straipsnio 2 dalyje nurodytus atvejus;** **2) Europos Komisijos priimtiems įgyvendinimo aktams, pagal šio straipsnio 3 dalyje nurodytas priemones nustatantiems techninius ir metodinius reikalavimus.** <...> **6. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo privalo užtikrinti, kad kibernetinio saugumo subjektas laikytųsi šiame įstatyme jam nustatytų pareigų, ir prižiūrėti jų laikymąsi. Kibernetinio saugumo subjekto vadovas, įgaliodamas šioje dalyje nurodytą asmenį, užtikrina, kad jis turėtų būtinų priemonių, reikalingų nurodytam įgaliojimui vykdyti.** **33 straipsnis. Esminio subjekto vadovo laikinas nušalinimas nuo pareigų** **1. Teismas, gavęs Nacionalinio kibernetinio saugumo centro prašymą, nutartimi turi teisę laikinai nušalinti esminio subjekto vadovą nuo pareigų, jeigu nustatoma, kad šio įstatymo 28 straipsnio 1 dalies 1–4 ir 6 punktuose numatytų vykdymo užtikrinimo priemonių taikymas yra neveiksmingas.** **2. Nacionalinis kibernetinio saugumo centras, prieš kreipdamasis į teismą su prašymu laikinai nušalinti esminio subjekto vadovą nuo pareigų šio straipsnio 1 dalyje nurodytu pagrindu, privalo esminį subjektą informuoti pateikdamas esminę informaciją apie teisės aktų nuostatas ir nustatytus faktinius duomenis, kurie sudaro laikino esminio subjekto vadovo nušalinimo nuo pareigų pagrindus, ir nustatyti terminą, kuris negali būti trumpesnis kaip 10 darbo dienų nuo pranešimo įteikimo dienos, per kurį esminis subjektas turi imtis būtinų veiksmų nustatytiems trūkumams pašalinti ar reikalavimams įvykdyti. Nacionalinis kibernetinio saugumo centras šio straipsnio 1 dalyje nustatytu pagrindu į teismą turi teisę kreiptis tik pasibaigus Nacionalinis kibernetinio saugumo centro nustatytam terminui ir esminiam subjektui nesiėmus nurodytų veiksmų.** **3. Nacionalinio kibernetinio saugumo centro prašyme teismui dėl esminio subjekto vadovo laikino nušalinimo nuo pareigų turi būti nurodyta:** **1) aplinkybės, įrodančios, kad šio įstatymo 28 straipsnio 1 dalies 1–4 ir 6 punktuose numatytų užtikrinimo priemonių taikymas yra neveiksmingas;**	

	2) aplinkybės, įrodančios, kad esminiam subjektui buvo nustatytas terminas trūkumams pašalinti ar reikalavimams įvykdyti, o esminis subjektas nesiėmė nurodytų veiksmų; **3) esminio subjekto, kurio vadovą prašoma laikinai nušalinti nuo pareigų, paaiškinimai, jeigu tokie buvo gauti.** **4. Nutartis, kuria esminio subjekto vadovas laikinai nušalinimas nuo pareigų, nedelsiant nusiunčiama jį į pareigas priimančiam subjektui.** **5. Nutartis esminio subjekto vadovui ar jo atstovui paskelbiama Civilinio proceso kodekso nustatyta tvarka.** **6. Nuo teismo nutarties laikinai nušalinti esminio subjekto vadovą nuo pareigų paskelbimo dienos nušalintas nuo pareigų fizinis asmuo neturi teisės atlikti savo funkcijų ir visi po tokio teismo sprendimo paskelbimo dienos jo priimti sprendimai yra negaliojantys.** **7. Laikinas esminio subjekto vadovo nušalinimas nuo pareigų negali trukti ilgiau kaip šešis mėnesius. Prireikus šios priemonės taikymas gali būti pratęstas dar iki trijų mėnesių. Pratęsimų skaičius neribojamas, bet visais atvejais nušalinimas nuo pareigų negali trukti ilgiau nei to reikia, kad būtų užtikrinamas šio įstatymo nuostatų laikymasis** **8. Nutartį laikinai nušalinti esminio subjekto vadovą nuo pareigų, taip pat nutartį pratęsti šios priemonės taikymo terminą per 5 darbo dienas nuo nutarties paskelbimo esminis subjektas ar nušalintas esminio subjekto vadovas gali apskųsti aukštesnės instancijos teismui. Šio teismo priimta nutartis yra galutinė ir neskundžiama.** **9. Teismas privalo panaikinti laikiną esminio subjekto vadovo nušalinimą nuo pareigų ar laikiną teisės užsiimti tam tikra veikla sustabdymą, kai ši priemonė pasidaro nebereikalinga ar Nacionalinis kibernetinio saugumo centras prašo panaikinti laikiną sustabdymą. Nacionalinis kibernetinio saugumo centras, gavęs motyvuotą nušalinto esminio subjekto vadovo prašymą ir nustatęs, kad esminio subjekto vadovo nušalinimas yra nebereikalingas, ne vėliau kaip per 7 darbo dienas nuo prašymo gavimo dienos, privalo prašyti teismo panaikinti laikiną sustabdymą** **10. Nacionalinis kibernetinio saugumo centras informaciją apie esminį subjektą, kurio vadovas laikinai nušalintas nuo pareigų, skelbia savo interneto svetainėje.** **ANK projektas**	

	„480 straipsnis. Lietuvos Respublikos kibernetinio saugumo įstatyme nustatytų kibernetinio saugumo užtikrinimo pareigų atlikimo pažeidimai **<...>** **3. Lietuvos Respublikos kibernetinio saugumo įstatyme nustatytų reikalavimų kibernetinio saugumo subjektų vadovams ar jų įgaliotiems asmenims pažeidimas** **užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar jų įgaliotiems asmenims nuo dviejų šimtų penkiasdešimt iki trijų tūkstančių eurų.** **4. Šio straipsnio 3 dalyje numatytas administracinis nusižengimas, padarytas pakartotinai,** **užtraukia baudą nuo dviejų tūkstančių iki šešių tūkstančių eurų.“**	
2. Valstybės narės užtikrina, kad esminių ir svarbių subjektų valdymo organų nariai turėtų dalyvauti mokymuose, ir skatina esminius ir svarbius subjektus reguliariai siūlyti panašius mokymus savo darbuotojams, kad jie įgytų pakankamai žinių ir įgūdžių, kad galėtų nustatyti riziką ir įvertinti kibernetinio saugumo rizikos valdymo praktiką bei jos poveikį subjekto teikiamoms paslaugoms.	**KSĮ projektas** **14 straipsnis. Kibernetinio saugumo rizikos valdymo priemonės** **<...>** **7. Kibernetinio saugumo subjekto valdymo organų nariai, vadovas ir jo įgaliotas asmuo, jeigu toks yra, ar kibernetinio saugumo subjektas, jei jis yra fizinis asmuo, privalo ne rečiau kaip kartą per 2 metus Nacionalinio kibernetinio saugumo centro vadovo nustatyta tvarka išklausyti kibernetinio saugumo mokymus bei užtikrinti kibernetinio saugumo subjekto darbuotojų nuolatinį švietimą kibernetinio saugumo srityje.**	Visiškas
21 straipsnis. Kibernetinio saugumo rizikos valdymo priemonės		
1. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai imtųsi tinkamų ir proporcingų techninių, operatyvinių ir organizacinių priemonių, siekdami valdyti tinklų ir informacinių sistemų, kurias tie subjektai naudoja savo veiklai arba teikdami savo paslaugas, saugumui kylančią riziką ir užkirsti kelią incidentų poveikiui jų paslaugų gavėjams ir kitoms paslaugoms arba juos sumažinti iki minimumo. Atsižvelgiant į naujausius technikos laimėjimus ir, kai taikytina, atitinkamus Europos ir tarptautinius standartus, taip pat į įgyvendinimo sąnaudas, pirmoje pastraipoje nurodytomis priemonėmis užtikrinamas toks tinklų ir informacinių sistemų saugumo lygis, kuris atitinka kilusią riziką. Vertinant tų priemonių proporcingumą, tinkamai atsižvelgiama į subjekto	**KSĮ projektas** **14 straipsnis. Kibernetinio saugumo rizikos valdymo priemonės** **1. Kibernetinio saugumo subjektai privalo užtikrinti šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus atitinkančiai veiklai vykdyti ar paslaugoms teikti naudojamų tinklų ir informacinių sistemų atitiktį kibernetinio saugumo rizikos valdymo priemonėms:** **1) kibernetinio saugumo reikalavimams, tvirtinamiems Vyriausybės, išskyrus šio straipsnio 2 dalyje nurodytus atvejus;** **2) Europos Komisijos priimtiems įgyvendinimo aktams, pagal šio straipsnio 3 dalyje nurodytas priemones nustatantiems techninius ir metodinius reikalavimus.** **2. Kibernetinio saugumo subjektai privalo šio straipsnio 1 dalies 1 punkte nurodytus kibernetinio saugumo reikalavimus įgyvendinti per Vyriausybės**	Visiškas

galimybės patirti riziką laipsnį, subjekto dydį ir incidentų tikimybę bei jų sunkumą, įskaitant jų socialinį ir ekonominį poveikį.	**nustatytą ne trumpesnį nei 12 mėn. terminą nuo jų įtraukimo į Kibernetinio saugumo subjektų registrą. Nustatydama terminą Vyriausybė privalo atsižvelgti į kibernetinio saugumo reikalavimams įgyvendinti reikalingus žmogiškuosius ir finansinius išteklius.** **<...>** **4. Specialusis subjektas privalo užtikrinti jų naudojamų tinklų ir informacinių sistemų atitiktį tik šio straipsnio 1 dalies 2 punkte nurodytiems teisės aktams.**	
2. 1 dalyje nurodytos priemonės grindžiamos visus pavojus apimančiu požiūriu, kuriuo siekiama apsaugoti tinklų ir informacines sistemas bei jų fizinę aplinką nuo incidentų, ir jos apima bent šiuos elementus: a) rizikos analizės ir informacinių sistemų saugumo politiką; b) incidentų valdymą; c) veiklos tęstinumą, pvz., atsarginių kopijų valdymą ir veiklos atkūrimą po ekstremaliųjų įvykių, ir krizių valdymą; d) tiekimo grandinės saugumą, įskaitant su saugumu susijusius aspektus, susijusius su kiekvieno subjekto ir jo tiesioginių tiekėjų ar paslaugų teikėjų santykiais; e) tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumą, įskaitant pažeidžiamumo valdymą ir atskleidimą; f) politiką ir procedūras, skirtas kibernetinio saugumo rizikos valdymo priemonių veiksmingumui įvertinti; g) pagrindinę kibernetinės higienos praktiką ir kibernetinio saugumo mokymus; h) kriptografijos ir, kai taikytina, šifravimo naudojimo politiką ir procedūras; i) žmogiškųjų išteklių saugumą, prieigos kontrolės politiką ir turto valdymą; j) kai taikytina, kelių veiksnių tapatumo nustatymo ar nuolatinio tapatumo nustatymo sprendimų, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių ryšių sistemų subjekto viduje naudojimą.	**KSĮ projektas** **14 straipsnis. Kibernetinio saugumo rizikos valdymo priemonės** **<...>** **5. Kibernetinio saugumo reikalavimai apima šiuos elementus:** **1) kibernetinio saugumo rizikos analizės, tinklų ir informacinių sistemų kibernetinio saugumo politiką;** **2) už kibernetinį saugumą atsakingų asmenų, nurodytų šio įstatymo 15 straipsnyje, ir kibernetinio saugumo subjekto vadovo ar jo įgalioto asmens pareigas;** **3) kibernetinių incidentų valdymą;** **4) veiklos tęstinumą;** **5) tiekimo grandinės saugumą, įskaitant aspektus, susijusius su kiekvieno kibernetinio saugumo subjekto ir jo tiesioginių tiekėjų ar paslaugų teikėjų santykius;** **6) tinklų ir informacinių sistemų įsigijimą, plėtojimą ir priežiūros saugumą, įskaitant spragų valdymą ir atskleidimą;** **7) politiką ir procedūras, skirtas kibernetinio saugumo reikalavimų veiksmingumui įvertinti;** **8) kibernetinės higienos praktiką ir reguliarius kibernetinio saugumo mokymus;** **9) kriptografijos ir šifravimo naudojimo politiką ir procedūras;** **10) žmogiškųjų išteklių saugumą, prieigos kontrolės politiką ir turto valdymą;** **11) kelių veiksnių tapatumo nustatymo ar nuolatinio tapatumo nustatymo sprendimų, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių ryšių sistemų subjekto viduje naudojimą;** **12) kibernetinio saugumo subjektų naudotojų, administratorių, tiekėjų, jų subtiekėjų ir kitų ūkio subjektų teisių ir prieigos prie kibernetinio saugumo**	Visiškas

	subjektų valdomų ir (ar) tvarkomų tinklų ir informacinių sistemų ir (ar) skaitmeninių duomenų suteikimo ir valdymo politiką; **13) kitus atskiriems sektoriams arba atskiroms kibernetinio saugumo subjektų grupėms taikomus kibernetinio saugumo reikalavimus, nustatytus atsižvelgiant į atskiruose sektoriuose identifikuotas kibernetinio saugumo rizikas.**	
3. Valstybės narės užtikrina, kad, subjektai, svarstydami, kurios šio straipsnio 2 dalies d punkte nurodytos priemonės yra tinkamos, atsižvelgtų į kiekvieno tiesioginio tiekėjo ir paslaugų teikėjo pažeidžiamumą ir į jų tiekėjų ir paslaugų teikėjų produktų bendrą kokybę ir kibernetinio saugumo praktiką, įskaitant jų saugumo plėtojimo procedūras. Valstybės narės taip pat užtikrina, kad subjektai, svarstydami, kurios tame punkte nurodytos priemonės yra tinkamos, privalėtų atsižvelgti į pagal 22 straipsnio 1 dalį atliktų koordinuojamų ypatingos svarbos tiekimo grandinių rizikos vertinimų rezultatus.	*Direktyvos 21 straipsnio 3 dalies įgyvendinimas nėra KSĮ projekto reguliavimo srityje. Lietuvos Respublikos krašto apsaugos ministerija numato parengti įgyvendinamąjį teisės aktą, kuriuo bus tvirtinamos kibernetinio saugumo rizikos valdymo priemonės*	Dalinis
4. Valstybės narės užtikrina, kad subjektas, kuris nustato, kad jis nesilaiko 2 dalyje numatytų priemonių, nepagrįstai nedelsdamas imtųsi visų būtinų, tinkamų ir proporcingų taisomųjų priemonių.	**KSĮ projektas** **26 straipsnis. Kibernetinio saugumo subjektų patikrinimai** **1. Nacionalinis kibernetinio saugumo centras atlieka kibernetinio saugumo subjektų atitikties šio įstatymo reikalavimams, išskyrus nustatytus šio įstatymo VI ir VII skyriuose, patikrinimus.** **2. Nacionalinis kibernetinio saugumo centras turi teisę pradėti šio straipsnio 1 dalyje nurodytą kibernetinio saugumo subjekto patikrinimą bet kokiu klausimu, susijusiu su šio įstatymo reikalavimais, nustatytais kibernetinio saugumo subjektams, kurių nevykdymas laikomas pažeidimu, savo iniciatyva, gavęs skundą ar kitų šaltinių pagrindu, išskyrus šio straipsnio 3 dalyje nurodytus atvejus.** **3. Šio straipsnio 1 dalyje nurodyti svarbių subjektų patikrinimai atliekami tik gavus duomenų ar informacijos, kad svarbus subjektas, kaip įtariama, padarė šio įstatymo reikalavimų pažeidimą.** **28 straipsnis. Vykdymo užtikrinimo priemonės** **1. Nacionalinis kibernetinio saugumo centras, šio įstatymo 26 straipsnio 1 dalyje nurodyto patikrinimo metu nustatęs šio įstatymo pažeidimą, taiko vykdymo užtikrinimo priemonę ar jų grupę:**	Visiškas

	1) teikia įspėjimus, kad kibernetinio saugumo subjektai pažeidžia šio įstatymo nustatytus reikalavimus; **2) duoda nurodymus esminiams subjektams dėl priemonių, kurių reikia siekiant užkirsti kelią kibernetiniam incidentui arba jam suvaldyti, ir tokių priemonių įgyvendinimo bei jų įgyvendinimo ataskaitų pateikimo terminų, nurodymus kibernetinio saugumo subjektams, kad atitinkami subjektai pašalintų nustatytus trūkumus arba ištaisytų šio įstatymo reikalavimų pažeidimus;** **3) duoda nurodymus kibernetinio saugumo subjektams nutraukti veiksmus, kurie pažeidžia šio įstatymo nustatytus reikalavimus, ir tokių veiksmų nebekartoti;** **4) duoda nurodymus kibernetinio saugumo subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų naudojamos kibernetinio saugumo rizikos valdymo priemonės atitiktų šio įstatymo 14 straipsnio 1 dalyje nurodytus teisės aktus arba kad jie įvykdytų šio įstatymo 18 straipsnio 1 dalyje nustatytą pareigą pranešti apie kibernetinius incidentus;** **5) duoda nurodymus kibernetinio saugumo subjektams informuoti fizinius arba juridinius asmenis, kuriems jie teikia paslaugas arba vykdo jiems aktualią veiklą ir kuriuos didelė kibernetinė grėsmė gali paveikti, apie grėsmės pobūdį, taip pat apie visus galimus veiksmus, kurių gali imtis tie fiziniai ar juridiniai asmenys, reaguodami į tą grėsmę;** **6) duoda nurodymus kibernetinio saugumo subjektams per pagrįstą terminą įgyvendinti kibernetinio saugumo audito metu pateiktas rekomendacijas;** **7) paskiria stebėsenos pareigūną, kuriam per nustatytą laikotarpį pavestos aiškiai apibrėžtos užduotys, prižiūrėti, kaip esminiai subjektai laikosi šio įstatymo 14 ir 18 straipsnių reikalavimų;** **8) duoda nurodymus kibernetinio saugumo subjektams konkrečiu būdu viešai paskelbti šio įstatymo pažeidimo aspektus;** **9) skiria kibernetinio saugumo subjektams baudą šio įstatymo 30 ir 31 straipsniuose nustatyta tvarka, kartu su bet kuriomis šios dalies 1–8, 10 ir 11 punktuose nurodytomis priemonėmis;** **10) inicijuoja šio įstatymo 32 straipsnyje nustatytą laikiną teisės užsiimti dalimi ar visa esminio subjekto vykdoma veikla ar teikti paslaugas sustabdymą;** **11) inicijuoja šio įstatymo 33 straipsnyje nustatytą esminio subjekto vadovo, išskyrus Lietuvos Respublikos Seimo, Vyriausybės ir Prezidento**	

	sprendimu skiriamus viešojo administravimo subjektų vadovus, laikiną nušalinimą nuo pareigų **2. Vykdymo užtikrinimo priemonės pritaikymas neatleidžia kibernetinio saugumo subjekto nuo pareigos, už kurios nevykdymą pritaikyta vykdymo užtikrinimo priemonė, atlikimo. Vykdymo užtikrinimo priemonės taikymas juridiniams asmenims neatleidžia jų vadovų ir darbuotojų nuo įstatymuose nustatytos civilinės, administracinės ar baudžiamosios atsakomybės.**	
5. Komisija ne vėliau kaip 2024 m. spalio 17 d. priima įgyvendinimo aktus, kuriais nustatomi 2 dalyje nurodytų priemonių techniniai ir metodiniai reikalavimai, taikomi DNS paslaugų teikėjams, aukščiausio lygio domenų vardų registrams, debesijos kompiuterijos paslaugų teikėjams, duomenų centrų paslaugų teikėjams, turinio teikimo tinklo teikėjams, valdomų paslaugų teikėjams, valdomų saugumo paslaugų teikėjams, elektroninių prekyviečių, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų ir patikimumo užtikrinimo paslaugų teikėjams. Komisija gali priimti įgyvendinimo aktus, kuriais nustatomi 2 dalyje nurodytų priemonių būtinieji techniniai ir metodiniai reikalavimai, taip pat sektoriams taikomi reikalavimai, taikomi kitiems esminiams ir svarbiems subjektams nei nurodytieji šios dalies pirmoje pastraipoje. Rengdama šios dalies pirmoje ir antroje pastraipose nurodytus įgyvendinimo aktus, Komisija, kiek įmanoma, laikosi Europos ir tarptautinių standartų bei atitinkamų techninių specifikacijų. Komisija keičiasi rekomendacijomis ir bendradarbiauja su Bendradarbiavimo grupe ir ENISA dėl įgyvendinimo aktų projektų pagal 14 straipsnio 4 dalies e punktą. Tie įgyvendinimo aktai priimami laikantis 39 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.	**KSĮ projektas** **14 straipsnis. Kibernetinio saugumo rizikos valdymo priemonės** **1. Kibernetinio saugumo subjektai privalo užtikrinti šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus atitinkančiai veiklai vykdyti ar paslaugoms teikti naudojamų tinklų ir informacinių sistemų atitiktį kibernetinio saugumo rizikos valdymo priemonėms:** **1) kibernetinio saugumo reikalavimams, tvirtinamiems Vyriausybės, išskyrus šio straipsnio 2 dalyje nurodytus atvejus;** **2) Europos Komisijos priimtiems įgyvendinimo aktams, pagal šio straipsnio 3 dalyje nurodytas priemones nustatantiems techninius ir metodinius reikalavimus.** <...> **4. Specialusis subjektas privalo užtikrinti jų naudojamų tinklų ir informacinių sistemų atitiktį tik šio straipsnio 1 dalies 2 punkte nurodytiems teisės aktams.**	Visiškas
22 straipsnis. Sąjungos lygmeniu koordinuojami ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimai		
1. Bendradarbiavimo grupė, bendradarbiaudama su Komisija ir ENISA, gali atlikti koordinuotus konkrečių ypatingos svarbos IRT paslaugų, IRT sistemų ar IRT produktų tiekimo grandinių	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	

saugumo rizikos vertinimus, atsižvelgdama į techninius ir, kai tinkama, netechninius rizikos veiksnius.		
2. Komisija, pasikonsultavusi su Bendradarbiavimo grupe ir ENISA bei prireikus su atitinkamais suinteresuotaisiais subjektais, nustato konkrečias ypatingos svarbos IRT paslaugas, IRT sistemas ar IRT produktus, dėl kurių gali būti atliekamas 1 dalyje nurodytas koordinuotas saugumo rizikos vertinimas.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
23 straipsnis. Pareigos pranešti		
1. Kiekviena valstybė narė užtikrina, kad esminiai ir svarbūs subjektai nepagrįstai nedelsdami praneštų valstybės narės CSIRT arba, kai taikytina, jos kompetentingai institucijai pagal 4 dalį apie bet kokį incidentą, darantį didelį poveikį jų paslaugų teikimui, kaip nurodyta 3 dalyje (toliau – didelis incidentas). Kai tinkama, atitinkami subjektai nepagrįstai nedelsdami praneša jų paslaugų gavėjams apie didelius incidentus, kurie gali turėti neigiamos įtakos tų paslaugų teikimui. Kiekviena valstybė narė užtikrina, kad tie subjektai, inter alia, praneštų visą informaciją, pagal kurią CSIRT arba, kai taikytina, kompetentinga institucija galėtų nustatyti tarpvalstybinį incidento poveikį. Vien dėl pranešimo veiksmo negali būti padidinama pranešančiojo subjekto atsakomybė. Jei atitinkami subjektai praneša kompetentingai institucijai apie didelį incidentą pagal pirmą pastraipą, valstybė narė užtikrina, kad ta kompetentinga institucija, gavusi pranešimą, perduotų jį CSIRT. Tarpvalstybinio arba tarpsektorinio didelio incidento atveju valstybės narės užtikrina, kad jų bendrieji kontaktiniai punktai laiku gautų atitinkamą informaciją, apie kurią pranešta pagal 4 dalį.	**KSĮ projektas** **18 straipsnis. Pranešimai apie kibernetinius incidentus** **1. Kibernetinio saugumo subjektai privalo pranešti Nacionaliniam kibernetinio saugumo centrui apie:** **1) didelį kibernetinį incidentą, darantį poveikį jų šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus atitinkančiai vykdomai veiklai ir (ar) teikiamoms paslaugoms;** **2) šios dalies 1 punkte nenurodytus kibernetinius incidentus, darančius poveikį jų šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus atitinkančiai vykdomai veiklai ir (ar) teikiamoms paslaugoms nacionalinio kibernetinių incidentų valdymo plano, tvirtinamo Vyriausybės, nustatytais terminais ir pateikiant Vyriausybės nustatytą informaciją.**	Visiškas
2. Kai taikytina, valstybės narės užtikrina, kad esminiai ir svarbūs subjektai nepagrįstai nedelsdami informuotų savo paslaugų gavėjus, kuriuos didelė kibernetinė grėsmė galėjo paveikti, apie visas priemones ar teisių gynimo priemones, kurių tie gavėjai gali imtis reaguodami į tą grėsmę. Atitinkamais atvejais subjektai taip pat praneša tiems gavėjams apie pačią didelę kibernetinę grėsmę.	**KSĮ projektas** **7 straipsnis. Nacionalinis kibernetinio saugumo centras** <...> **2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:** <...>	Dalinis

	12) kai būtina informuoti visuomenę siekiant išvengti kibernetinio incidento arba valdyti vykstantį kibernetinį incidentą arba iškilusią kibernetinę grėsmę, prieš tai pasikonsultavęs su kibernetinio saugumo subjektu, pranešusiu apie kibernetinį incidentą, informuoja visuomenę apie kibernetinį incidentą ir (ar) kibernetinę grėsmę, jeigu įmanoma, nurodydamas veiksmus, kurių būtina imtis reaguojant į tą kibernetinį incidentą ir (ar) kibernetinę grėsmę, arba reikalauja, kad tai padarytų informaciją pateikęs kibernetinio saugumo subjektas; **28 straipsnis. Vykdymo užtikrinimo priemonės** **1. Nacionalinis kibernetinio saugumo centras, šio įstatymo 26 straipsnio 1 dalyje nurodyto patikrinimo metu nustatęs šio įstatymo pažeidimą, taiko vykdymo užtikrinimo priemonę ar jų grupę:** **<...>** **5) duoda nurodymus kibernetinio saugumo subjektams informuoti fizinius arba juridinius asmenis, kuriems jie teikia paslaugas arba vykdo jiems aktualią veiklą ir kuriuos didelė kibernetinė grėsmė gali paveikti, apie grėsmės pobūdį, taip pat apie visus galimus veiksmus, kurių gali imtis tie fiziniai ar juridiniai asmenys, reaguodami į tą grėsmę.**	
3. Incidentas laikomas dideliu, jeigu: a) dėl jo atitinkamas subjektas patyrė arba gali patirti didelių paslaugų teikimo sutrikimų arba finansinių nuostolių; b) jis paveikė arba gali paveikti kitus fizinius ar juridinius asmenis sukeldamas didelę turtinę arba neturtinę žalą.	**KSĮ projektas** **18 straipsnis. Pranešimai apie kibernetinius incidentus** **1. Kibernetinio saugumo subjektai privalo pranešti Nacionaliniam kibernetinio saugumo centrui apie:** **1) didelį kibernetinį incidentą, darantį poveikį jų šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus atitinkančiai vykdomai veiklai ir (ar) teikiamoms paslaugoms;** **2) šios dalies 1 punkte nenurodytus kibernetinius incidentus, darančius poveikį jų šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus atitinkančiai vykdomai veiklai ir (ar) teikiamoms paslaugoms nacionalinio kibernetinių incidentų valdymo plano, tvirtinamo Vyriausybės, nustatytais terminais ir pateikiant Vyriausybės nustatytą informaciją.** **2. Kibernetinis incidentas laikomas dideliu bent vienu iš šių atvejų:** **1) jeigu dėl kibernetinio incidento atitinkamas subjektas patyrė arba gali patirti didelių paslaugų teikimo sutrikimų arba finansinių nuostolių;** **2) jeigu kibernetinis incidentas paveikė arba gali paveikti kitus fizinius ar juridinius asmenis, sukeldamas didelę turtinę arba neturtinę žalą.**	Visiškas

	3. Išsamūs, kai kibernetinis incidentas laikomas dideliu, apibrėžiami Europos Komisijos priimamuose įgyvendinimo aktuose.	
4. Valstybės narės užtikrina, kad 1 dalyje nurodyto pranešimo tikslais atitinkami subjektai CSIRT arba, kai taikytina, kompetentingai institucijai pateiktų: a) nepagrįstai nedelsdami ir bet kuriuo atveju per 24 valandas nuo tada, kai sužinojo apie didelį incidentą, – ankstyvąjį perspėjimą, kuriame, kai taikytina, nurodoma, ar didelį incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai ir ar jis galėtų daryti tarpvalstybinį poveikį; b) nepagrįstai nedelsdami ir bet kuriuo atveju per 72 valandas nuo tada, kai sužinojo apie didelį incidentą, – pranešimą apie incidentą, kuriame, kai taikytina, atnaujinama a) punkte nurodyta informacija ir nurodomas didelio incidento, įskaitant jo sunkumą ir poveikį, pradinis vertinimas, taip pat nurodomi užvaldymo rodikliai, jei tokių yra; c) CSIRT arba, kai taikytina, kompetentingos institucijos prašymu – tarpinę ataskaitą apie atitinkamus atnaujintus duomenis apie padėtį; d) ne vėliau kaip per vieną mėnesį nuo b punkte nurodyto pranešimo apie incidentą – galutinę ataskaitą, kurioje pateikiama ši informacija: i) išsamus incidento, įskaitant jo sunkumą ir poveikį, aprašymas; ii) grėsmės arba pagrindinės priežasties, dėl kurios incidentas galėjo būti sukeltas, rūšis; iii) taikomos ir įgyvendinamos poveikio mažinimo priemonės; iv) kai taikytina, tarpvalstybinis incidento poveikis; e) tuo atveju, jei d punkte nurodytos galutinės ataskaitos pateikimo metu incidentas tebevyksta, valstybės narės užtikrina, kad atitinkami subjektai tuo metu pateiktų pažangos ataskaitą, o galutinę ataskaitą – per vieną mėnesį nuo tada, kai suvaldė incidentą. Nukrypstant nuo pirmos pastraipos b punkto, patikimumo užtikrinimo paslaugų teikėjas didelių incidentų, darančių poveikį jo patikimumo užtikrinimo paslaugų teikimui, atveju nepagrįstai nedelsdamas ir bet kuriuo atveju per 24 valandas nuo tada, kai	**KSĮ projektas** **18 straipsnis. Pranešimai apie kibernetinius incidentus** **<...>** **4. Pranešant apie didelį kibernetinį incidentą pateikiama:** **1) nedelsiant, bet ne vėliau kaip per 24 valandas nuo sužinojimo apie didelį kibernetinį incidentą – ankstyvasis perspėjimas, kuriame pagal galimybes nurodoma, ar didelį kibernetinį incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai ir ar jis galėtų daryti tarpvalstybinį poveikį;** **2) nedelsiant, bet ne vėliau kaip per 72 valandas nuo sužinojimo apie didelį kibernetinį incidentą – pranešimas apie kibernetinį incidentą, kuriame pagal galimybes atnaujinama šios dalies 1 punkte nurodyta informacija ir nurodomas didelio kibernetinio incidento, įskaitant jo sunkumą ir poveikį, pradinis vertinimas, taip pat nurodomi įsilaužimo įrodymai, jei tokių yra;** **3) Nacionalinio kibernetinio saugumo centro prašymu – tarpinė atitinkamų atnaujintų padėties duomenų ataskaita per Nacionalinio kibernetinio saugumo centro nurodytą pateikimo terminą;** **4) ne vėliau kaip per vieną mėnesį nuo šios dalies 1 punkte nurodyto pranešimo apie kibernetinį incidentą – galutinė ataskaita, kurioje pateikiama ši informacija:** **a) išsamus kibernetinio incidento, įskaitant jo sunkumą ir poveikį, aprašymas;** **b) grėsmės arba pagrindinės priežasties, dėl kurios kibernetinis incidentas galėjo būti sukeltas, rūšis;** **c) taikomos ir įgyvendinamos kibernetinio incidento poveikio mažinimo priemonės;** **d) tarpvalstybinis kibernetinio incidento poveikis, jeigu toks buvo;** **5) tuo atveju, jei šios dalies 4 punkte nurodytos galutinės ataskaitos pateikimo metu kibernetinis incidentas tebevyksta, pateikiama pažangos ataskaita, o galutinė ataskaita – per vieną mėnesį nuo tada, kai kibernetinis incidentas suvaldomas.** **5. Kibernetinio saugumo subjektai privalo pranešti apie kibernetinį incidentą ir kibernetinę grėsmę nacionalinio kibernetinių incidentų valdymo plano, tvirtinamo Vyriausybės, nustatyta tvarka.**	Visiškas

sužinojo apie didelį incidentą, apie tai praneša CSIRT arba, kai taikytina, kompetentingai institucijai.		
5. CSIRT arba kompetentinga institucija nepagrįstai nedelsdama ir, kai įmanoma, – per 24 valandas nuo 4 dalies a punkte nurodyto ankstyvojo perspėjimo gavimo pateikia atsakymą pranešančiajam subjektui, įskaitant pirminę grįžtamąją informaciją apie didelį incidentą, ir, subjekto prašymu – galimų rizikos mažinimo priemonių įgyvendinimo gaires arba operacinių patarimų. Jei CSIRT nėra pradinis 1 dalyje nurodyto pranešimo gavėjas, gaires teikia kompetentinga institucija, bendradarbiaudama su CSIRT. CSIRT teikia papildomą techninę pagalbą, jei to prašo atitinkamas subjektas. Jei įtariama, kad didelis incidentas yra baudžiamojo pobūdžio, CSIRT arba kompetentinga institucija taip pat teikia gaires dėl pranešimo apie didelį incidentą teisėsaugos institucijoms.	**KSĮ projektas** **18 straipsnis. Pranešimai apie kibernetinius incidentus** <...> **6. Nacionaliniame kibernetinių incidentų valdymo plane nustatoma:** **1) terminai per kuriuos turi būti pranešama apie šio straipsnio 1 dalies 1 punkte nenurodytus kibernetinius incidentus;** **2) informacija, kuri turi būti perduodama pranešant apie šio straipsnio 1 dalies 1 punkte nenurodytus kibernetinius incidentus;** **3) informacijos apie kibernetinius incidentus pateikimo būdai ir priemonės;** **4) institucijų veiksmai, gavus informaciją apie kibernetinius incidentus;** **5) išsamesni atvejai, kada kibernetinis incidentas laikomas dideliu, jeigu išsamesni atvejai nenustatomi Europos Komisijos įgyvendinimo aktuose.** *Pastaba: Detalesnius institucijų veiksmus, gavus informacijos apie kibernetinius incidentus, numatoma aprašyti Nacionaliniame kibernetinių incidentų valdymo plane*	Dalinis
6. Kai taikytina ir visų pirma tuomet, kai didelis incidentas yra susijęs su dviem ar daugiau valstybių narių, CSIRT, kompetentinga institucija arba bendrasis kontaktinis punktas nepagrįstai nedelsdami informuoja apie didelį incidentą kitas paveiktas valstybes nares, ir ENISA. Tokia informacija apima pagal 4 dalį gautos informacijos rūšį. Tai darydami CSIRT, kompetentinga institucija ar bendrasis kontaktinis punktas, laikydamiesi Sąjungos arba nacionalinės teisės, saugo subjekto saugumo ir komercinius interesus, taip pat pateiktos informacijos konfidencialumą.		
7. Kai visuomenės informuotumas yra būtinas siekiant užkirsti kelią dideliam incidentui ar reaguoti į besitęsiantį didelį incidentą arba kai didelio incidento atskleidimas kitais atvejais atitinka viešąjį interesą, valstybės narės CSIRT arba, kai taikytina, jos kompetentinga institucija ir atitinkamais atvejais kitų atitinkamų valstybių narių CSIRT arba kompetentingos institucijos, gali, pasikonsultavusios su atitinkamu subjektu, informuoti visuomenę apie incidentą arba pareikalauti, kad tą padarytų subjektas.		

8. CSIRT arba kompetentingos institucijos prašymu bendrasis kontaktinis punktas perduoda pagal 1 dalį gautus pranešimus kitų paveiktų valstybių narių bendriesiems kontaktiniams punktams.	*Detalesnius institucijų veiksmus, gavus informacijos apie kibernetinius incidentus, numatoma aprašyti Nacionaliniame kibernetinių incidentų valdymo plane*	Dalinis
9. Bendrasis kontaktinis punktas kas tris mėnesius teikia ENISA suvestinę ataskaitą, į kurią įtraukiami nuasmeninti ir suvestiniai duomenys apie didelius incidentus, incidentus, kibernetines grėsmes ir vos neįvykusius incidentus, apie kuriuos pranešta pagal šio straipsnio 1 dalį ir pagal 30 straipsnį. Siekdama prisidėti prie palyginamos informacijos teikimo ENISA gali priimti technines gaires dėl į suvestinę ataskaitą įtrauktos informacijos parametrų. ENISA kas šešis mėnesius informuoja Bendradarbiavimo grupę ir CSIRT tinklą apie savo išvadas dėl gautų pranešimų.	*Detalesnius institucijų veiksmus, gavus informacijos apie kibernetinius incidentus, numatoma aprašyti Nacionaliniame kibernetinių incidentų valdymo plane*	Dalinis
10. CSIRT arba, kai taikytina, kompetentingos institucijos teikia kompetentingoms institucijoms pagal Direktyvą (ES) 2022/2557 informaciją apie didelius incidentus, incidentus, kibernetines grėsmes ir vos neįvykusius incidentus, apie kuriuos pagal šio straipsnio 1 dalį ir 30 straipsnį pranešė subjektai, identifikuoti kaip ypatingos svarbos subjektai pagal Direktyvą (ES) 2022/2557	*Detalesnius institucijų veiksmus, gavus informacijos apie kibernetinius incidentus, numatoma aprašyti Nacionaliniame kibernetinių incidentų valdymo plane*	Dalinis
11. Komisija gali priimti įgyvendinimo aktus, kuriais išsamiau nustatoma pagal šio straipsnio 1 dalį ir 30 straipsnį pateikiamo pranešimo ir pagal šio straipsnio 2 dalį pateikiamos informacijos rūšis, formatas ir procedūra. Komisija ne vėliau kaip 2024 m. spalio 17 d. priima įgyvendinimo aktus dėl DNS paslaugų teikėjų, aukšto lygio domenų vardų registrų, debesijos kompiuterijos paslaugų teikėjų, duomenų centrų paslaugų teikėjų, turinio teikimo tinklo teikėjų, valdomų paslaugų teikėjų, valdomų saugumo paslaugų teikėjų, taip pat elektroninių prekyviečių, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų teikėjų, kuriais išsamiau apibrėžiami atvejai, kuriais incidentas laikomas dideliu, kaip nurodyta 3 dalyje. Komisija gali priimti tokius įgyvendinimo aktus dėl kitų esminių ir svarbių subjektų.	**KSĮ projektas** **18 straipsnis. Pranešimai apie kibernetinius incidentus** **<...>** **6. Nacionaliniame kibernetinių incidentų valdymo plane nustatoma:** **1) terminai per kuriuos turi būti pranešama apie šio straipsnio 1 dalies 1 punkte nenurodytus kibernetinius incidentus;** **2) informacija, kuri turi būti perduodama pranešant apie šio straipsnio 1 dalies 1 punkte nenurodytus kibernetinius incidentus;** **3) informacijos apie kibernetinius incidentus pateikimo būdai ir priemonės;** **4) institucijų veiksmai, gavus informaciją apie kibernetinius incidentus;** **5) išsamesni atvejai, kada kibernetinis incidentas laikomas dideliu, jeigu išsamesni atvejai nenustatomi Europos Komisijos įgyvendinimo aktuose.**	Visiškas

Komisija keičiasi rekomendacijomis ir bendradarbiauja su Bendradarbiavimo grupe dėl šios dalies pirmoje ir antroje pastraipose nurodytų įgyvendinimo aktų projektų pagal 14 straipsnio 4 dalies e punktą. Tie įgyvendinimo aktai priimami laikantis 39 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.		
24 straipsnis. Europos kibernetinio saugumo sertifikavimo schemų naudojimas		
1. Siekdamos įrodyti atitiktį tam tikriems 21 straipsnio reikalavimams, valstybės narės gali reikalauti, kad esminiai ir svarbūs subjektai naudotų konkrečius esminių ar svarbių subjektų sukurtus arba iš trečiųjų šalių nupirktus IRT produktus, IRT paslaugas ir IRT procesus, kurie sertifikuoti pagal Europos kibernetinio saugumo sertifikavimo schemas, priimtas pagal Reglamento (ES) 2019/881 49 straipsnį. Be to, valstybės narės skatina esminius ir svarbius subjektus naudotis kvalifikuotomis patikimumo užtikrinimo paslaugomis.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
2. Komisijai pagal 38 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, kuriais ši direktyva papildoma nustatant, kokių kategorijų esminiai ir svarbūs subjektai privalo naudoti tam tikrus sertifikuotus IRT produktus, IRT paslaugas ir IRT procesus arba gauti sertifikatą pagal Europos kibernetinio saugumo sertifikavimo schemą, priimtą pagal Reglamento (ES) 2019/881 49 straipsnį. Tie deleguotieji aktai priimami tais atvejais, kai nustatomi nepakankami kibernetinio saugumo lygiai, ir į tuos aktus įtraukiamas įgyvendinimo laikotarpis. Prieš priimdama tokius deleguotuosius aktus, Komisija atlieka poveikio vertinimą ir vykdo konsultacijas pagal Reglamento (ES) 2019/881 56 straipsnį.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
3. Kai šio straipsnio 2 dalies tikslais nėra tinkamos Europos kibernetinio saugumo sertifikavimo schemos, Komisija, pasikonsultavusi su Bendradarbiavimo grupe ir Europos kibernetinio saugumo sertifikavimo grupe, gali prašyti ENISA parengti potencialią schemą pagal Reglamento (ES) 2019/881 48 straipsnio 2 dalį.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	

25 straipsnis. Standartizacija		
1. Siekdamos skatinti vienodą 21 straipsnio 1 ir 2 dalių įgyvendinimą, valstybės narės, nereikalaudamos taikyti kokios nors konkrečios rūšies technologijos ir nesuteikdamos jai pirmenybės, skatina naudotis Europos ir tarptautiniais standartais ir techninėmis specifikacijomis, kurie yra svarbūs tinklų ir informacinių sistemų saugumui.	**KSĮ projektas** **3 straipsnis. Kibernetinio saugumo principai** **1. Kibernetinis saugumas grindžiamas šiais kibernetinio saugumo principais:** <...> **5) standartizacijos ir technologinio neutralumo – įgyvendinant kibernetinio saugumo rizikos valdymo priemones, kibernetinio saugumo subjektai skatinami vadovautis nacionaliniais, Europos Sąjungos ir kitais tarptautiniais tinklų ir informacinių sistemų saugumo standartais ir techninėmis specifikacijomis, nereikalaujant taikyti kokios nors konkrečios rūšies technologijos ir nesuteikiant jai pirmenybės.**	Visiškas
2. ENISA, bendradarbiaudama su valstybėmis narėmis ir, kai tikslinga, pasikonsultavusi su atitinkamais suinteresuotaisiais subjektais, parengia rekomendacijas ir gaires dėl techninių sričių, kurios turi būti apsvarstytos atsižvelgiant į 1 dalį, taip pat dėl jau galiojančių standartų, be kita ko, nacionalinių standartų, kuriuose būtų numatyta įtraukti tas sritis.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
26 straipsnis. Jurisdikcija ir teritoriškumas		
1. Laikoma, kad subjektai, patenkantys į šios direktyvos taikymo sritį, laikomi priklausančiais valstybės narės, kurioje jie yra įsisteigę, jurisdikcijai, išskyrus: a) viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjus, kurie laikomi priklausančiais valstybės narės, kurioje jie teikia savo paslaugas, jurisdikcijai; b) DNS paslaugų teikėjus, aukščiausio lygio domenų vardų registrus, domenų vardų registravimo paslaugas teikiančius subjektus, debesijos kompiuterijos paslaugų teikėjus, duomenų centrų paslaugų teikėjus, turinio teikimo tinklo paslaugų teikėjus, valdomų paslaugų teikėjus, valdomų saugumo paslaugų teikėjus, taip pat elektroninių prekyviečių, interneto paieškos sistemų ar socialinio tinklo paslaugų platformų paslaugų teikėjus, kurie laikomi priklausančiais valstybės narės, kurioje yra jų pagrindinė buveinė Sąjungoje, jurisdikcijai;	**KSĮ projektas** **12 straipsnis. Jurisdikcija ir teritoriškumas** **1. Identifikuojant kibernetinio saugumo subjektus laikoma, kad Lietuvos Respublikos jurisdikcijai priklauso:** **1) asmenys, registruoti ar įsisteigę Lietuvos Respublikoje, išskyrus:** **a) viešojo administravimo subjektus, kurie yra įsteigti kitos valstybės;** **b) šios dalies 3 punkte nurodyti subjektai, kurių pagrindinė buveinė yra ne Lietuvos Respublikoje;** **2) viešojo administravimo subjektai, kuriuos Lietuvos Respublika įsteigė kitose valstybėse;** **3) DNS paslaugų teikėjai, aukščiausio lygio domenų vardų registro paslaugas teikiantys subjektai, domenų vardų registravimo paslaugas teikiantys subjektai, debesijos kompiuterijos paslaugų teikėjai, duomenų centrų paslaugų teikėjai, turinio teikimo tinklo paslaugų teikėjai, valdomų paslaugų teikėjai, valdomų saugumo paslaugų teikėjai, elektroninių prekyviečių, interneto paieškos**	Visiškas

c) viešojo administravimo subjektus, kurie laikomi priklausančiais valstybės narės, kuri juos įsteigė, jurisdikcijai.	**sistemų ar socialinio tinklo paslaugų platformų paslaugų teikėjai, kurių pagrindinė buveinė yra Lietuvos Respublikoje;** **4) viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjai, teikiantys šias paslaugas Lietuvos Respublikoje.**	
2. Šios direktyvos tikslais laikoma, kad 1 dalies b punkte nurodyto subjekto pagrindinė buveinė Sąjungoje yra valstybėje narėje, kurioje daugiausia priimami su kibernetinio saugumo rizikos valdymo priemonėmis susiję sprendimai. Jei tokios valstybės narės neįmanoma nustatyti arba jei tokie sprendimai nepriimami Sąjungoje, laikoma, kad pagrindinė buveinė yra valstybėje narėje, kurioje vykdomos kibernetinio saugumo operacijos. Jei tokios valstybės narės neįmanoma nustatyti, laikoma, kad pagrindinė buveinė yra valstybėje narėje, kurioje atitinkamas subjektas turi padalinį, kuriame dirba daugiausia darbuotojų Sąjungoje.	**KSĮ projektas** **12 straipsnis. Jurisdikcija ir teritoriškumas** <...> **2. Laikoma, kad šio straipsnio 1 dalies 3 punkte nurodyta pagrindinė buveinė yra Lietuvos Respublikoje, jeigu šio straipsnio 1 dalies 3 punkte nurodyti subjektai yra registruoti ar įsisteigę Lietuvos Respublikoje. Laikoma, kad šio straipsnio 1 dalies 3 punkte nurodyta pagrindinė buveinė yra Lietuvos Respublikoje, jeigu su kibernetinio saugumo rizikos valdymo priemonėmis susiję sprendimai yra priimami Lietuvos Respublikoje. Jeigu Europos Sąjungos valstybė, kurioje priimami tokie sprendimai, nenustatoma arba tokie sprendimai Europos Sąjungoje nepriimami, laikoma, kad pagrindinė buveinė yra Lietuvos Respublikoje, kai Lietuvos Respublikoje įgyvendinamos kibernetinio saugumo rizikos valdymo priemonės. Jeigu nenustatoma Europos Sąjungos valstybė, kurioje įgyvendinamos kibernetinio saugumo rizikos valdymo priemonės, laikoma, kad pagrindinė buveinė yra Lietuvos Respublikoje, jeigu subjektas Lietuvos Respublikoje turi padalinį, kuriame dirba daugiausia jo darbuotojų Europos Sąjungoje.**	Visiškas
3. Jei 1 dalies b punkte nurodytas subjektas nėra įsisteigęs Sąjungoje, bet teikia paslaugas Sąjungoje, jis paskiria atstovą Sąjungoje. Atstovas turi būti įsisteigęs vienoje iš tų valstybių narių, kuriose siūlomos paslaugos. Laikoma, kad toks subjektas priklauso valstybės narės, kurioje yra įsisteigęs jo atstovas, jurisdikcijai. Jei Sąjungoje nėra pagal šią dalį paskirto atstovo, bet kuri valstybė narė, kurioje subjektas teikia paslaugas, gali imtis teisinių veiksmų prieš subjektą dėl šios direktyvos pažeidimo.	**KSĮ projektas** **12 straipsnis. Jurisdikcija ir teritoriškumas** <...> **3. 3. Jei šio straipsnio 1 dalies 3 punkte nurodytas subjektas nėra įsisteigęs Europos Sąjungoje, bet teikia paslaugas Lietuvos Respublikoje, jis privalo paskirti Europos Sąjungoje įsisteigusį fizinį arba juridinį asmenį, paskirtą veikti tik DNS paslaugų teikėjo, aukščiausio lygio domenų vardų registro paslaugas teikiančio subjekto, domenų vardų registravimo paslaugas teikiančio subjekto, debesijos kompiuterijos paslaugų teikėjo, duomenų centro paslaugų teikėjo, turinio teikimo tinklo paslaugų teikėjo, valdomų paslaugų teikėjo, valdomų saugumo paslaugų teikėjo, elektroninės prekyvietės paslaugų teikėjo, interneto paieškos sistemos paslaugų teikėjo arba socialinio tinklo paslaugų platformų paslaugų teikėjo, kuris nėra įsisteigęs Europos Sąjungoje, vardu, į kurį Nacionalinis kibernetinio saugumo centras gali kreiptis vietoj subjekto dėl to subjekto pareigų pagal šį įstatymą (toliau – atstovas) Europos Sąjungoje. Šioje**	Visiškas

	dalyje nurodytas atstovas turi būti įsisteigęs vienoje iš tų valstybių narių, kuriose siūlomos paslaugos. Jei šio straipsnio 1 dalies 3 punkte nurodytas subjektas skiria atstovą Lietuvos Respublikoje arba jo nepaskiria, bet teikia paslaugas Lietuvos Respublikoje, laikoma, kad toks subjektas priklauso Lietuvos Respublikos jurisdikcijai.	
4. 1 dalies b punkte nurodyto subjekto atstovo paskyrimu nedaromas poveikis teisiniams veiksmams, kurie galėtų būti inicijuoti prieš patį subjektą.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
5. Valstybės narės, gavusios savitarpio pagalbos prašymą dėl 1 dalies b punkte nurodyto subjekto, gali, neviršydamos to prašymo ribų, imtis tinkamų priežiūros ir vykdymo užtikrinimo priemonių, susijusių su atitinkamu subjektu, teikiančiu paslaugas arba turinčiu tinklų ir informacinę sistemą jų teritorijoje.	**KSĮ projektas** **21 straipsnis. Savitarpio pagalba** **1. Nacionalinis kibernetinio saugumo centras, gavęs kitos valstybės narės kompetentingos institucijos pagrįstą savitarpio prašymą, vykdo šio įstatymo 26 ir 28 straipsniuose numatytus kibernetinio saugumo subjektų patikrinimo ir (ar) vykdymo užtikrinimo priemonių veiksmus, taip pat kitus prašomus veiksmus, kuriuos vykdyti suteikia teisę šis įstatymas. Teikdamas savitarpio pagalbą dėl šio įstatymo 12 straipsnio 1 dalies 3 punkte nurodyto subjekto, kurio pagrindinė buveinė yra ne Lietuvos Respublikoje, Nacionalinis kibernetinio saugumo centras negali imtis daugiau veiksmų, nei nurodyta savitarpio pagalbos prašyme.** **2. Nacionalinis kibernetinio saugumo centras kitos valstybės narės kompetentingos institucijos savitarpio pagalbos prašymą gali atmesti tik tais atvejais kai:** **1) Nacionalinis kibernetinio saugumo centras neturi kompetencijos teikti prašomą pagalbą;** **2) prašoma pagalba nėra proporcinga Nacionalinio kibernetinio saugumo centro turimiems žmogiškiesiems ar finansiniams ištekliams;** **3) prašymas yra susijęs su informacija arba apima veiklą, kurios atskleidimas arba atlikimas prieštarautų Lietuvos Respublikos nacionaliniam saugumui, visuomenės saugumui ar gynybai.** **3. Jeigu Nacionalinis kibernetinio saugumo centras pagal kompetenciją negali įgyvendinti pateikto savitarpio pagalbos prašymo, tačiau nustatęs, kad prašymą turėtų vykdyti kita valstybės institucija, prašymo nenagrinėja, persiunčia jį kitai valstybės institucijai ir apie tai praneša prašymą pateikusiai kitos valstybės kompetentingai institucijai.** **4. Nacionalinis kibernetinio saugumo centras negalėdamas įvykdyti kitos valstybės narės kompetentingos institucijos savitarpio pagalbos prašymo apie tai privalo ją informuoti, nurodydamas negalėjimo įgyvendinti prašymo priežastis,**	Visiškas

	ir, jeigu yra kitos valstybės narės prašymas, prieš atmesdamas tokį prašymą, konsultuojasi su Europos Komisija ir (ar) Europos Sąjungos kibernetinio saugumo agentūra.	
27 straipsnis. Subjektų registras		
1. ENISA sukuria ir tvarko DNS paslaugų teikėjų, aukščiausio lygio domenų vardų registrų, domenų vardų registravimo paslaugas teikiančių subjektų, debesijos kompiuterijos paslaugų teikėjų, duomenų centrų paslaugų teikėjų, turinio teikimo tinklo paslaugų teikėjų, valdomų paslaugų teikėjų, valdomų saugumo paslaugų teikėjų, taip pat internetinių prekyviečių, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų paslaugų teikėjų registrą, remdamasi iš bendrųjų kontaktinių punktų pagal 4 dalį gauta informacija. Gavusi prašymą, ENISA suteikia kompetentingoms institucijoms prieigą prie to registro, kartu, kai taikytina, užtikrindama informacijos konfidencialumo apsaugą.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	

2. Valstybės narės reikalauja, kad 1 dalyje nurodyti subjektai kompetentingoms institucijoms ne vėliau kaip 2025 m. sausio 17 d. pateiktų šią informaciją: a) subjekto pavadinimą; b) I arba II priede nurodytą atitinkamą sektorių, subsektorių ir subjekto rūšį, jei taikoma; c) subjekto pagrindinės buveinės adresą ir kitus juridinius padalinius Sąjungoje arba, jei jie nėra įsisteigę Sąjungoje, pagal 26 straipsnio 3 dalį paskirto atstovo adresą; d) naujausius kontaktinius duomenis, įskaitant subjekto ir, kai taikytina, pagal 26 straipsnio 3 dalį paskirto jo atstovo el. pašto adresus ir telefono numerius; e) valstybes nares, kuriose subjektas teikia paslaugas, ir f) subjekto IP adresų ruožus.	**KSĮ projektas** **11 straipsnis. Kibernetinio saugumo subjektai** **1. Kibernetinio saugumo subjekto statusą įgyja ir Kibernetinio saugumo subjektų registre registruojami asmenys, atitinkantys bent vieną iš šio straipsnio 3–5 dalyse nurodytų bendrųjų ar specialiųjų kibernetinio saugumo subjektų identifikavimo kriterijų ir šiuose kriterijuose nurodytoms paslaugoms teikti ar veiklai vykdyti valdantys ir (ar) tvarkantys tinklų ir informacines sistemas. Atsižvelgiant į galimą neigiamą poveikį, kurį kibernetinis incidentas gali padaryti kibernetinio saugumo subjektų valdomoms ir (ar) tvarkomoms tinklų ir informacinėms sistemoms, kibernetinio saugumo subjektai skirstomi į esminius kibernetinio saugumo subjektus (toliau – esminiai subjektai) ir svarbius kibernetinio saugumo subjektus (toliau – svarbūs subjektai).** **2. Kibernetinio saugumo subjektai įgyja pareigas, numatytas kibernetinio saugumo subjektams, tik nuo jų įregistravimo Kibernetinio saugumo subjektų registre.** **3. Bendrieji esminių subjektų identifikavimo kriterijai:** **<...>** **2) subjektas šio įstatymo 1 priede nurodytame skaitmeninės infrastruktūros sektoriuje teikia kvalifikuotas patikimumo užtikrinimo paslaugas, aukščiausio lygio .lt domeno vardų registravimo paslaugas ar domenų vardų sistemos (toliau – DNS) paslaugas, išskyrus šakninių vardų serverių operatorius;** **4. Bendrieji svarbių subjektų identifikavimo kriterijai:** **<...>** **6) subjektas teikia domenų vardų registravimo paslaugas.** **13 straipsnis. Kibernetinio saugumo subjektų registras** **<...>** **3. Kibernetinio saugumo subjektų registrą sudaro šie pagrindiniai duomenys apie kibernetinio saugumo subjektus:** **1) jeigu kibernetinio saugumo subjektas yra juridinis asmuo – kibernetinio saugumo subjekto pavadinimas, juridinio asmens kodas, teisinis statusas, ekonominės veiklos forma, pagrindinės buveinės adresas (jeigu kibernetinio saugumo subjektas nėra įsisteigęs Europos Sąjungoje – pagal šio įstatymo 12 straipsnio 3 dalį paskirto atstovo pavadinimas, teisinis statusas, ekonominės veiklos forma, registracijos numeris, kontaktiniai duomenys**	Visiškas

	(elektroninio pašto adresas, ryšio numeris ir adresas) ir kitų juridinių padalinių Europos Sąjungoje adresai, jei kibernetinio saugumo subjektas yra DNS paslaugų teikėjas, aukščiausio lygio domenų vardų registro paslaugas teikiantis subjektas, debesijos kompiuterijos paslaugų teikėjas, duomenų centrų paslaugų teikėjas, turinio teikimo tinklo paslaugų teikėjas, valdomų paslaugų teikėjas, valdomų saugumo paslaugų teikėjas, internetines prekyvietes, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų paslaugų teikėjas (toliau – specialusis subjektas) ar yra domenų vardų registravimo paslaugas teikiantis subjektas; **2) jeigu kibernetinio saugumo subjektas yra fizinis asmuo – kibernetinio saugumo subjekto vardas, pavardė, asmens kodas, veiklos vykdymo adresas;** **3) kibernetinio saugumo subjekto kontaktiniai duomenys (elektroninio pašto adresas, ryšio numeris);** **4) kibernetinio saugumo subjekto teikiamos paslaugos ir (ar) vykdomos veiklos, atitinkančios šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus;** **5) kibernetinio saugumo subjekto naudojami interneto protokolo (IP) adresų rėžiai;** **6) valstybės, kuriose kibernetinio saugumo subjektas teikia paslaugas ir (ar) vykdo veiklą, nurodytą šio įstatymo 1 ir 2 prieduose nurodytuose sektoriuose ir subsektoriuose;** **7) kibernetinio saugumo subjekto paslaugų teikimui ar veiklai reikšmingos tinklų ir informacinės sistemos;** **8) šio įstatymo 1 ir 2 prieduose nurodytas sektorius, kuriame kibernetinio saugumo subjektas veikia ar teikia paslaugas, subsektorius, subjekto rūšis kibernetinio saugumo subjekto sektorius, subsektorius, subjekto rūšis.** **4. Subjektas, atitinkantis šio įstatymo 11 straipsnio 3-5 dalyse nustatytus kibernetinio saugumo subjektų identifikavimo kriterijus, Kibernetinio saugumo subjektų registro duomenų tvarkytojui pateikia duomenis, nurodytus Kibernetinio saugumo informacinio tinklo nuostatuose, tvirtinamuose Krašto apsaugos ministerijos. Duomenys teikiami šiuose nuostatuose nustatyta tvarka.** **5. Kibernetinio saugumo subjektus registruoja ir išregistruoja Kibernetinio saugumo informacinio tinklo duomenų tvarkytojas Kibernetinio saugumo informacinio tinklo nuostatuose nustatyta tvarka.**	

3. Valstybės narės užtikrina, kad 1 dalyje nurodyti subjektai nedelsdami ir bet kuriuo atveju ne vėliau kaip per tris mėnesius nuo pakeitimo dienos praneštų kompetentingai institucijai apie bet kokius jų pagal 2 dalį pateiktos informacijos pakeitimus.	*Kibernetinio saugumo subjektų, įskaitant nurodytus 3 dalyje, pranešimo pareigos bus aprašytos Kibernetinio saugumo informacinio tinklo nuostatuose.*	
4. Gavęs 2 ir 3 dalyse nurodytą informaciją, išskyrus 2 dalies f punkte nurodytą informaciją, atitinkamos valstybės narės bendrasis kontaktinis punktas, nepagrįstai nedelsdamas ją persiunčia ENISA.	*Detalesnius institucijų veiksmus, numatoma aprašyti Kibernetinio saugumo informacinio tinklo nuostatuose*	
5. Kai taikytina, šio straipsnio 2 ir 3 dalyse nurodyta informacija teikiama naudojantis 3 straipsnio 4 dalies ketvirtoje pastraipoje nurodytu nacionaliniu mechanizmu.	*Detalesnius institucijų veiksmus, numatoma aprašyti Kibernetinio saugumo informacinio tinklo nuostatuose*	
28 straipsnis. Domenų vardų registracijos duomenų bazė		
1. Siekdamos prisidėti prie DNS saugumo, stabilumo ir atsparumo, valstybės narės reikalauja, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai rūpestingai rinktų ir specialioje duomenų bazėje saugotų tikslius ir išsamius domenų vardų registracijos duomenis, laikydamiesi Sąjungos duomenų apsaugos teisės aktų dėl duomenų, kurie yra asmens duomenys.	**KSĮ projektas** **17 straipsnis. Reikalavimai aukščiausio lygio domenų vardų registro ir domenų vardų registravimo paslaugų teikimui** **Kibernetinio saugumo subjektai, kurie yra aukščiausio lygio domenų vardų registro paslaugas teikiantys subjektai ir domenų vardų registravimo paslaugas teikiantys subjektai, privalo:** **1) siekdami prisidėti prie domenų vardų sistemos saugumo, stabilumo ir atsparumo, kaupti informaciją, pagal kurią būtų galima nustatyti domenų vardų turėtojus ir kontaktinius asmenis, administruojančius aukščiausio lygio domenų vardais pažymėtus domenų vardus, ir su jais susisiekti,** laikydamiesi Reglamento (ES) 2016/679 reikalavimų, kai tvarkomi asmens duomenys**. Tokia informacija apima:** **a) domeno vardą;** **b) registracijos datą;** **c) domeno vardo turėtojo juridinio asmens pavadinimą ar fizinio asmens vardą ir pavardę, ir kontaktinius duomenis (elektroninio pašto adresas, ryšio numeris);** **d) domeno vardą administruojančio kontaktinio asmens elektroninio pašto adresą ir ryšio numerį, jei jie skiriasi nuo domeno vardo turėtojo duomenų.** **2) taikyti politiką ir procedūras, įskaitant tikrinimo procedūras, kuriomis užtikrinama, kad domenų vardų registracijos duomenų bazėje būtų pateikiama tiksli ir išsami informacija;**	Visiškas
2. 1 dalies tikslais valstybės narės reikalauja, kad domenų vardų registracijos duomenų bazėse būtų būtina informacija, pagal kurią būtų galima nustatyti domenų vardų turėtojus ir kontaktinius punktus, administruojančius aukščiausio lygio domenų vardais pažymėtus domenų vardus, ir su jais susisiekti. Tokia informacija apima: a) domeno vardą; b) registracijos datą; c) registruotojo pavadinimą, pavardę, kontaktinį el. pašto adresą ir telefono numerį; d) domeno vardą administruojančio kontaktinio punkto el. pašto adresą ir telefono numerį, jei jie skiriasi nuo registruotojo duomenų.		
3. Valstybės narės reikalauja, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai taikytų politiką ir procedūras, įskaitant tikrinimo		

procedūras, kuriomis užtikrinama, kad 1 dalyje nurodytose duomenų bazėse būtų pateikiama tiksli ir išsami informacija. Valstybės narės reikalauja, kad tokia politika ir procedūros būtų skelbiamos viešai.	**3) skelbti šio straipsnio 2 ir 5 punktuose nurodytą politiką ir procedūras viešai savo interneto svetainėse ar, jeigu jie interneto svetainės neturi, kitomis visuomenės informavimo priemonėmis;** **4) nepagrįstai nedelsdami po domeno vardo užregistravimo paskelbti viešai interneto svetainėse ar, jeigu jie interneto svetainės neturi, kitomis visuomenės informavimo priemonėmis domeno vardo registracijos duomenis, kurie nėra asmens duomenys;** **5) gavę teisėtus ir tinkamai pagrįstus teisėtos prieigos prie domenų vardų registracijos duomenų, kurie yra asmens duomenys, prašančių asmenų prašymus, pagal taikomą duomenų atskleidimo politiką ir procedūras suteikti prieigą prie konkrečių domenų vardų registracijos duomenų, laikydamiesi Reglamento (ES) 2016/679 nustatytos tvarkos. Atsakymai prašančiam subjektui turi būti teikiami nepagrįstai nedelsiant ir bet kuriuo atveju ne vėliau kaip per 72 valandas nuo tada, kai gaunamas prašymas suteikti prieigą;** **6) siekdami nedubliuoti domenų vardų registracijos duomenų rinkimo, bendradarbiauti tarpusavyje.**	
4. Valstybės narės reikalauja, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai nepagrįstai nedelsdami po domeno vardo užregistravimo viešai paskelbtų domeno vardo registracijos duomenis, kurie nėra asmens duomenys.		
5. Valstybės narės reikalauja, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai, gavę teisėtus ir tinkamai pagrįstus teisėtų prieigos prašančių subjektų prašymus, suteiktų prieigą prie konkrečių domenų vardų registracijos duomenų, laikydamiesi Sąjungos duomenų apsaugos teisės aktų. Valstybės narės reikalauja, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai, atsakytų nepagrįstai nedelsdami ir bet kuriuo atveju per 72 valandas nuo tada, kai gaunamas prašymas suteikti prieigą. Valstybės narės reikalauja, kad tokių duomenų atskleidimo politika ir procedūros būtų skelbiamos viešai.		
6. Dėl to, kad laikomasi 1–5 dalyse nustatytų pareigų, neturi būti dubliuojamas domenų vardų registracijos duomenų rinkimas. Tuo tikslu valstybės narės reikalauja, kad aukščiausio lygio domenų vardų registrai ir domenų vardų registravimo paslaugas teikiantys subjektai bendradarbiautų tarpusavyje.		
29 straipsnis. Dalijimosi kibernetinio saugumo informacija susitarimai		
1. Valstybės narės užtikrina, kad subjektai, patenkantys į šios direktyvos taikymo sritį, ir, kai tinkama, kiti subjektai, nepatenkantys į šios direktyvos taikymo sritį, galėtų savanoriškai tarpusavyje keistis svarbia kibernetinio saugumo informacija, įskaitant informaciją, susijusią su kibernetinėmis grėsmėmis, vos neįvykusiais incidentais, pažeidžiamumais, metodais ir procedūromis, užvaldymo rodikliais, priešiška taktika, konkrečių	**KSĮ projektas** **19 straipsnis. Kibernetinio saugumo informacinis tinklas** **<...>** **3. Kibernetinio saugumo informaciniu tinklo naudotojai yra asmenys, kurie atitinka Kibernetinio saugumo informacinio tinklo nuostatuose nurodytus reikalavimus. Šio straipsnio 1 dalies 6 punkte nustatytus nurodymus duodančios institucijos ir juos įgyvendinantys kibernetinio saugumo subjektai privalo**	Visiškas

grėsmių ir dalyvių informacija, kibernetinio saugumo įspėjimais ir rekomendacijomis dėl kibernetinio saugumo priemonių konfigūracijos siekiant aptikti kibernetinius išpuolius, kai tokiu dalijimusi informacija: a) siekiama užkirsti kelią incidentams, juos atskleisti, į juos reaguoti ar po jų atstatyti veiklą, arba sumažinti jų poveikį; b) didinamas kibernetinis saugumas, visų pirma didinant informuotumą apie kibernetines grėsmes, ribojant arba sustabdant tokių grėsmių plitimo galimybes, remiant įvairius gynybos pajėgumus, pažeidžiamumų ištaisymą ir atskleidimą, grėsmių nustatymo, sustabdymo ir prevencijos metodus, švelninimo strategijas ar reagavimo ir veiklos atstatymo etapus, arba skatinant viešųjų ir privačiųjų subjektų atliekamus bendradarbiavimu grindžiamus kibernetinių grėsmių mokslinius tyrimus.	**naudotis Kibernetinio saugumo informacinio tinklo dalimi, kurioje tvarkomi duomenys apie privalomus nurodymus blokuoti domeno vardą, identifikuojantį interneto svetainę, nepriklausomai nuo kibernetinio saugumo subjektų atitikties Kibernetinio saugumo informacinio tinklo nuostatuose nurodytiems reikalavimams.** **4. Kibernetinio saugumo subjektai turi teisę tapti Kibernetinio saugumo informacinio tinklo naudotojais, įgyvendindami tarpusavio dalijimosi kibernetinio saugumo informacija susitarimus. Nepriklausomai nuo to, ar naudojamasi Kibernetinio saugumo informaciniu tinklu, kibernetinio saugumo subjektai privalo pranešti Nacionaliniam kibernetinio saugumo centrui apie tokių susitarimų sudarymą, taip pat apie pasitraukimą iš tokių susitarimų per 20 darbo dienų nuo šių aplinkybių atsiradimo.**	
2. Valstybės narės užtikrina, kad informacija būtų keičiamasi esminių ir svarbių subjektų ir, kai tinkama, jų tiekėjų ar paslaugų teikėjų bendruomenėse. Toks keitimasis vykdomas taikant dalijimosi kibernetinio saugumo informacija susitarimus, susijusius su galimai neskelbtina informacija, kuria dalijamasi.		
3. Valstybės narės sudaro palankesnes sąlygas sudaryti šio straipsnio 2 dalyje nurodytus dalijimosi kibernetinio saugumo informacija susitarimus. Tokiuose susitarimuose gali būti nustatyti veiklos elementai, įskaitant specialių IT platformų ir automatizavimo priemonių naudojimą, dalijimosi informacija susitarimų turinys ir sąlygos. Nustatydamos išsamią informaciją apie valdžios institucijų dalyvavimą tokiuose susitarimuose, valstybės narės gali nustatyti sąlygas dėl informacijos, kurią turi pateikti kompetentingos institucijos arba CSIRT. Valstybės narės teikia pagalbą tokių susitarimų taikymui pagal 7 straipsnio 2 dalies h punkte nurodytą savo politiką.		
4. Valstybės narės užtikrina, kad esminiai ir svarbūs subjektai kompetentingoms institucijoms praneša apie savo dalyvavimą 2 dalyje nurodytuose dalijimosi informacija susitarimuose		

sudarydami tokius susitarimus arba, kai tinkama, apie pasitraukimą iš tokių susitarimų, kai toks pasitraukimas įsigalioja.		
5. ENISA teikia pagalbą sudarant 2 dalyje nurodytų dalijimosi kibernetinio saugumo informacija susitarimus, teikdama geriausios praktikos pavyzdžius ir gaires.	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	
30 straipsnis. Savanoriškas pranešimas apie svarbią informaciją		
1. Valstybės narės užtikrina, kad, be 23 straipsnyje numatytos pranešimų teikimo pareigos, pranešimus CSIRT arba, kai taikytina, kompetentingoms institucijoms, savanoriškai galėtų teikti: a) esminiai ir svarbūs subjektai apie incidentus, kibernetines grėsmes ir vos neįvykusius incidentus; b) kiti nei a punkte nurodyti subjektai, nepriklausomai nuo to, ar jie patenka į šios direktyvos taikymo sritį – apie didelius incidentus, kibernetines grėsmes ir vos neįvykusius incidentus.	**KSĮ projektas** **24 straipsnis. Savanoriškas pranešimas** **1. Asmenys, kuriems šio įstatymo 18 straipsnio 1 dalyje nėra nustatytos pareigos pranešti apie kibernetinius incidentus, kibernetines grėsmes, vos neįvykusius kibernetinius incidentus ir (ar) taikytas kibernetinių incidentų valdymo priemones, turi teisę savanoriškai apie juos pranešti Nacionaliniam kibernetinio saugumo centrui. Nacionalinis kibernetinio saugumo centras tokius pranešimus tvarko Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka.**	Visiškas
2. Valstybės narės tvarko šio straipsnio 1 dalyje nurodytus pranešimus laikydamosi procedūros, nustatytos 23 straipsnyje. Valstybės narės gali teikti pirmenybę privalomų pranešimų tvarkymui, palyginti su savanoriškais pranešimais. Prireikus CSIRT ir, kai taikytina, kompetentingos institucijos teikia bendriesiems kontaktiniams punktams informaciją apie pagal šį straipsnį gautus pranešimus, kartu užtikrindamos pranešimą teikiančio subjekto pateiktos informacijos konfidencialumą ir tinkamą apsaugą. Nedarant poveikio nusikalstamų veikų prevencijai, tyrimui, jų atskleidimui ir baudžiamajam persekiojimui už jas, dėl savanoriško pranešimo pranešimą teikiančiam subjektui nenustatoma jokių papildomų pareigų, kurios jam nebūtų taikomos, jei jis nebūtų pateikęs pranešimo.	**KSĮ projektas** **24 straipsnis. Savanoriškas pranešimas** **<...>** **2. Asmeniui, savanoriškai pranešusiam apie kibernetinį incidentą, kibernetinę grėsmę, vos neįvykusį kibernetinį incidentą ir (ar) taikytas kibernetinių incidentų valdymo priemones, nenustatoma pareigų, susijusių su pranešimo pateikimu.**	Visiškas
31 straipsnis. Bendrieji aspektai, susiję su priežiūra ir vykdymo užtikrinimu		
1. Valstybės narės užtikrina, kad jų kompetentingos institucijos veiksmingai vykdytų priežiūrą ir imtųsi priemonių, būtinų siekiant užtikrinti, kad būtų laikomasi šios direktyvos.	**KSĮ projektas** **26 straipsnis. Kibernetinio saugumo subjektų patikrinimai**	Visiškas

	1. Nacionalinis kibernetinio saugumo centras atlieka kibernetinio saugumo subjektų atitikties šio įstatymo reikalavimams, išskyrus nustatytus šio įstatymo VI ir VII skyriuose, patikrinimus. **2. Nacionalinis kibernetinio saugumo centras turi teisę pradėti šio straipsnio 1 dalyje nurodytą kibernetinio saugumo subjekto patikrinimą bet kokiu klausimu, susijusiu su šio įstatymo reikalavimais, nustatytais kibernetinio saugumo subjektams, kurių nevykdymas laikomas pažeidimu, savo iniciatyva, gavęs skundą ar kitų šaltinių pagrindu, išskyrus šio straipsnio 3 dalyje nurodytus atvejus.** **3. Šio straipsnio 1 dalyje nurodyti svarbių subjektų patikrinimai atliekami tik gavus duomenų ar informacijos, kad svarbus subjektas, kaip įtariama, padarė šio įstatymo reikalavimų pažeidimą.** **4. Šio straipsnio 1 dalyje nurodyti patikrinimai atliekami šio įstatymo 27 straipsnyje ir Nacionalinio kibernetinio saugumo centro nustatyta tvarka. Nacionalinio kibernetinio saugumo centro nustatytame patikrinimų atlikimo tvarkos apraše turi būti numatoma kibernetinio saugumo rizikos požiūriu prioritetinių patikrinimų nustatymo tvarka.** **28 straipsnis. Vykdymo užtikrinimo priemonės** **1. Nacionalinis kibernetinio saugumo centras, šio įstatymo 26 straipsnio 1 dalyje nurodyto patikrinimo metu nustatęs šio įstatymo pažeidimą, taiko vykdymo užtikrinimo priemonę ar jų grupę:** **1) teikia įspėjimus, kad kibernetinio saugumo subjektai pažeidžia šio įstatymo nustatytus reikalavimus;** **2) duoda nurodymus esminiams subjektams dėl priemonių, kurių reikia siekiant užkirsti kelią kibernetiniam incidentui arba jam suvaldyti, ir tokių priemonių įgyvendinimo bei jų įgyvendinimo ataskaitų pateikimo terminų, nurodymus kibernetinio saugumo subjektams, kad atitinkami subjektai pašalintų nustatytus trūkumus arba ištaisytų šio įstatymo reikalavimų pažeidimus;** **3) duoda nurodymus kibernetinio saugumo subjektams nutraukti veiksmus, kurie pažeidžia šio įstatymo nustatytus reikalavimus, ir tokių veiksmų nebekartoti;** **4) duoda nurodymus kibernetinio saugumo subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų naudojamos kibernetinio saugumo rizikos valdymo priemonės atitiktų šio įstatymo 14 straipsnio 1 dalyje nurodytus**	

	teisės aktus arba kad jie įvykdytų šio įstatymo 18 straipsnio 1 dalyje nustatytą pareigą pranešti apie kibernetinius incidentus; **5) duoda nurodymus kibernetinio saugumo subjektams informuoti fizinius arba juridinius asmenis, kuriems jie teikia paslaugas arba vykdo jiems aktualią veiklą ir kuriuos didelė kibernetinė grėsmė gali paveikti, apie grėsmės pobūdį, taip pat apie visus galimus veiksmus, kurių gali imtis tie fiziniai ar juridiniai asmenys, reaguodami į tą grėsmę;** **6) duoda nurodymus kibernetinio saugumo subjektams per pagrįstą terminą įgyvendinti kibernetinio saugumo audito metu pateiktas rekomendacijas;** **7) paskiria stebėsenos pareigūną, kuriam per nustatytą laikotarpį pavestos aiškiai apibrėžtos užduotys, prižiūrėti, kaip esminiai subjektai laikosi šio įstatymo 14 ir 18 straipsnių reikalavimų;** **8) duoda nurodymus kibernetinio saugumo subjektams konkrečiu būdu viešai paskelbti šio įstatymo pažeidimo aspektus;** **9) skiria kibernetinio saugumo subjektams baudą šio įstatymo 30 ir 31 straipsniuose nustatyta tvarka, kartu su bet kuriomis šios dalies 1–8, 10 ir 11 punktuose nurodytomis priemonėmis;** **10) inicijuoja šio įstatymo 32 straipsnyje nustatytą laikiną teisės užsiimti dalimi ar visa esminio subjekto vykdoma veikla ar teikti paslaugas sustabdymą;** **11) inicijuoja šio įstatymo 33 straipsnyje nustatytą esminio subjekto vadovo, išskyrus Lietuvos Respublikos Seimo, Vyriausybės ir Prezidento sprendimu skiriamus viešojo administravimo subjektų vadovus, laikiną nušalinimą nuo pareigų** **2. Vykdymo užtikrinimo priemonės pritaikymas neatleidžia kibernetinio saugumo subjekto nuo pareigos, už kurios nevykdymą pritaikyta vykdymo užtikrinimo priemonė, atlikimo. Vykdymo užtikrinimo priemonės taikymas juridiniams asmenims neatleidžia jų vadovų ir darbuotojų nuo įstatymuose nustatytos civilinės, administracinės ar baudžiamosios atsakomybės.** **3. Taikydamas bet kurią iš šio straipsnio 1 dalyje nurodytų vykdymo užtikrinimo priemonių, Nacionalinis kibernetinio saugumo centras atsižvelgia į kiekvieno konkretaus atvejo aplinkybes, taip pat į:** **1) atsakomybę lengvinančias aplinkybes, nustatytas šio straipsnio 4 dalyje, atsakomybę sunkinančias aplinkybes, nustatytas šio straipsnio 5 dalyje, ir pažeistų nuostatų pavojingumą, nurodytą šio įstatymo 29 straipsnyje;** **2) pažeidimo trukmę;**	

	3) subjekto įvykdytus ankstesnius šio įstatymo pažeidimus per pastaruosius 2 metus; **4) padarytą turtinę arba neturtinę žalą, kuri vertinama apskaičiuojant finansinius ar ekonominius nuostolius, poveikį kitoms paslaugoms ir paveiktų naudotojų skaičių, nuostolių atlyginimą ar padaryto neigiamo poveikio panaikinimo;** **5) priemones, kurių subjektas ėmėsi siekdamas užkirsti kelią turtinei ar neturtinei žalai arba ją sumažinti;** **6) patvirtintų elgesio kodeksų arba patvirtintų sertifikavimo mechanizmų laikymąsi;** **7) bendradarbiavimą su Nacionaliniu kibernetinio saugumo centru;** **8) pažeidimo mastą.** **4. Šio straipsnio 3 dalies 1 punkte nurodytomis atsakomybę lengvinančiomis aplinkybėmis laikoma:** **1) subjektas savo noru užkirto kelią turtinei ar neturtinei žalai;** **2) subjektas atlygino padarytą žalą;** **3) subjektas pripažino pažeidimą ir padėjo Nacionaliniam kibernetinio saugumo centrui patikrinimo metu;** **4) subjektas savo valia nutraukė pažeidimą;** **5) pažeidimas padarytas dėl neatsargumo;** **6) subjekto, kuris yra ūkio subjektas, finansinė padėtis yra labai sunki.** **5. Šio straipsnio 3 dalies 1 punkte nurodytomis atsakomybę sunkinančiomis aplinkybėmis laikoma:** **1) pažeidimas padarytas pakartotinai.Laikoma, kad pažeidimas padarytas pakartotinai, jeigu subjektas, įtariamas pažeidimo padarymu, per paskutinius 12 mėnesių nuo sprendimo, kuriuo buvo paskirta vykdymo užtikrinimo priemonė, įsigaliojimo dienos padarė tokį patį pažeidimą. Padarius pakartotinį pažeidimą, šioje dalyje nustatytas terminas skaičiuojamas iš naujo;** **2) padarytas pavojingas pažeidimas, kaip jis suprantamas pagal šio įstatymo 29 straipsnio 2 dalį;** **3) subjektas neištaisė trūkumų pagal Nacionalinio kibernetinio saugumo centro pateiktus nurodymus;** **4) subjektas trukdė vykdyti kibernetinio saugumo audito ar stebėsenos pareigūno veiklą, kurią įpareigojo atlikti Nacionalinis kibernetinio saugumo centras, nustatęs pažeidimą;**	

	5) subjektas pateikė neteisingą informaciją, susijusios su šio įstatymo reikalavimais; **6) subjektas slėpė padarytą pažeidimą ar pažeidimą tęsė nepaisant to, kad Nacionalinis kibernetinio saugumo centras buvo atkreipęs dėmesį į pažeidimus ar veiklos trūkumus;** **7) pažeidimas padarytas tyčia.** **6. Šio straipsnio 1 dalyje nurodytos vykdymo užtikrinimo priemonės taikomos Vyriausybės nustatyta vykdymo užtikrinimo priemonių taikymo tvarka.** **7. Sprendimas dėl vykdymo užtikrinimo priemonės skyrimo gali būti priimtas, jeigu praėjo ne daugiau kaip 2 metai nuo pažeidimo dienos (išskyrus atvejus, kai sprendimo dėl vykdymo užtikrinimo priemonės skyrimo metu pažeidimas ar trūkumas jau yra ištaisytas), o kai pažeidimas trunkamasis – nuo jo paaiškėjimo dienos.**	
2. Valstybės narės gali leisti savo kompetentingoms institucijoms nustatyti užduočių prioritetus priežiūros srityje. Prioritetai nustatomi vadovaujantis rizika grindžiamu požiūriu. Tuo tikslu, vykdydamos savo priežiūros užduotis, numatytas 32 ir 33 straipsniuose, kompetentingos institucijos gali nustatyti priežiūros metodikas, pagal kurias būtų galima nustatyti tokių užduočių prioritetus, laikantis rizika grindžiamo požiūrio.	**KSĮ projektas** **26 straipsnis. Kibernetinio saugumo subjektų patikrinimai** **<...>** **4. Šio straipsnio 1 dalyje nurodyti patikrinimai atliekami šio įstatymo 27 straipsnyje ir Nacionalinio kibernetinio saugumo centro nustatyta tvarka. Nacionalinio kibernetinio saugumo centro nustatytame patikrinimų atlikimo tvarkos apraše turi būti numatoma kibernetinio saugumo rizikos požiūriu prioritetinių patikrinimų nustatymo tvarka.**	Visiškas
3. Kompetentingos institucijos, nagrinėdamos incidentus, dėl kurių pažeidžiamas asmens duomenų saugumas, glaudžiai bendradarbiauja su priežiūros institucijomis pagal Reglamentą (ES) 2016/679, nedarant poveikio priežiūros institucijų kompetencijai ir užduotims pagal tą reglamentą.	**KSĮ projektas** **20 straipsnis. Tarpinstitucinis bendradarbiavimas** **<...>** **2. Nacionalinis kibernetinio saugumo centras:** **<...>** **3) nustatęs, kad esminis ar svarbus subjektas gali būti padaręs asmens duomenų saugumo pažeidimą, apie tai nepagrįstai nedelsiant, bet ne vėliau kaip per 72 valandas nuo šios aplinkybės nustatymo, informuoja Valstybinę duomenų apsaugos inspekciją nurodydamas turimą informaciją apie Reglamento (ES) 2016/679 33 straipsnio 3 dalyje nurodytas aplinkybes.**	Visiškas
4. Nedarant poveikio nacionalinėms teisėkūros ir institucinėms sistemoms, valstybės narės užtikrina, kad, vykdydamos priežiūrą, kaip viešojo administravimo subjektai laikosi šios direktyvos, ir	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*	

taikydamos vykdymo užtikrinimo priemones šios direktyvos pažeidimų atveju, kompetentingos institucijos turėtų atitinkamus įgaliojimus vykdyti tokias užduotis naudodamosi veiklos nepriklausomumu nuo prižiūrimų viešojo administravimo subjektų. Valstybės narės gali nuspręsti dėl tinkamų, proporcingų ir veiksmingų priežiūros ir vykdymo užtikrinimo priemonių nustatymo tų subjektų atžvilgiu pagal nacionalines teisines ir institucines sistemas.		
32 straipsnis. Esminių subjektų priežiūros ir vykdymo užtikrinimo priemonės		
1. Valstybės narės užtikrina, kad priežiūros ar vykdymo užtikrinimo priemonės, taikomos esminiams subjektams šioje direktyvoje nustatytų pareigų atžvilgiu, būtų veiksmingos, proporcingos ir atgrasomos, atsižvelgiant į kiekvieno konkretaus atvejo aplinkybes.	**Viešojo administravimo įstatymas** **3 straipsnis. Viešojo administravimo principai** Viešojo administravimo subjektai savo veikloje vadovaujasi šiais principais: <...> 3) efektyvumo. Šis principas reiškia, kad viešojo administravimo subjektas, priimdamas ir įgyvendindamas sprendimus, jam skirtus išteklius naudoja kuo mažesnėmis sąnaudomis ir siekia geriausio rezultato; <...> 10) proporcingumo. Šis principas reiškia, kad administracinio sprendimo mastas ir jo įgyvendinimo priemonės turi atitikti būtinus ir pagrįstus administravimo tikslus. **KSĮ projektas** **28 straipsnis. Vykdymo užtikrinimo priemonės** **<...>** **3. Taikydamas bet kurią iš šio straipsnio 1 dalyje nurodytų vykdymo užtikrinimo priemonių, Nacionalinis kibernetinio saugumo centras atsižvelgia į kiekvieno konkretaus atvejo aplinkybes, taip pat į:** **1) atsakomybę lengvinančias aplinkybes, nustatytas šio straipsnio 4 dalyje, atsakomybę sunkinančias aplinkybės, nustatytas šio straipsnio 5 dalyje, ir pažeistų nuostatų pavojingumą, nurodytą šio įstatymo 29 straipsnyje;** **2) pažeidimo trukmę;** **3) subjekto įvykdytus ankstesnius šio įstatymo pažeidimus per pastaruosius 2 metus;** **4) padarytą turtinę arba neturtinę žalą, kuri vertinama apskaičiuojant finansinius ar ekonominius nuostolius, poveikį kitoms paslaugoms ir paveiktų**	Visiškas

	naudotojų skaičių, nuostolių atlyginimą ar padaryto neigiamo poveikio panaikinimo; **5) priemones, kurių subjektas ėmėsi siekdamas užkirsti kelią turtinei ar neturtinei žalai arba ją sumažinti;** **6) patvirtintų elgesio kodeksų arba patvirtintų sertifikavimo mechanizmų laikymąsi;** **7) bendradarbiavimą su Nacionaliniu kibernetinio saugumo centru;** **8) pažeidimo mastą.** **30 straipsnis. Baudos** **<...>** **4. Nustatomas konkretus baudos dydis turi būti veiksmingas, proporcingas padarytam pažeidimui ir atgrasantis nuo pažeidimų darymo ateityje. Nustatant konkretų baudos dydį atsižvelgiama į 28 straipsnio 3 dalyje nurodytas aplinkybes, išskyrus 28 straipsnio 4 dalies 2 punkte nurodytą aplinkybę.**	
2. Valstybės narės užtikrina, kad kompetentingos institucijos, vykdydamos savo priežiūros užduotis, susijusias su esminiais subjektais, turėtų bent šiuos įgaliojimus taikyti tiems subjektams: a) atlikti patikrinimus vietoje ir priežiūrą ne vietoje, įskaitant atsitiktinius patikrinimus, kuriuos atlieka apmokyti specialistai; b) atlikti reguliarius ir tikslinius saugumo auditus, kuriuos vykdo nepriklausoma įstaiga arba kompetentinga institucija; c) atlikti ad hoc auditus, be kita ko, kai tai pateisinama dėl didelio incidento arba esminio subjekto padaryto šios direktyvos pažeidimo atveju; d) atlikti saugumo patikrinimus, pagrįstus objektyviais, nediskriminaciniais, sąžiningais ir skaidriais rizikos vertinimo kriterijais, bendradarbiaudamos, kai to reikia, su atitinkamu subjektu; e) prašyti pateikti informaciją, būtiną atitinkamo subjekto priimtoms kibernetinio saugumo rizikos valdymo priemonėms įvertinti, įskaitant dokumentais pagrįstą kibernetinio saugumo politiką, taip pat informacijos teikimo pareigos kompetentingoms institucijoms pagal 27 straipsnį laikymąsi; f) prašyti leisti susipažinti su duomenimis, dokumentais ir informacija, reikalinga jų priežiūros užduotims atlikti;	**KSĮ projektas** **28 straipsnis. Vykdymo užtikrinimo priemonės** **1. Nacionalinis kibernetinio saugumo centras, šio įstatymo 26 straipsnio 1 dalyje nurodyto patikrinimo metu nustatęs šio įstatymo pažeidimą, taiko vykdymo užtikrinimo priemonę ar jų grupę:** **1) teikia įspėjimus, kad kibernetinio saugumo subjektai pažeidžia šio įstatymo nustatytus reikalavimus;** **2) duoda nurodymus esminiams subjektams dėl priemonių, kurių reikia siekiant užkirsti kelią kibernetiniam incidentui arba jam suvaldyti, ir tokių priemonių įgyvendinimo bei jų įgyvendinimo ataskaitų pateikimo terminų, nurodymus kibernetinio saugumo subjektams, kad atitinkami subjektai pašalintų nustatytus trūkumus arba ištaisytų šio įstatymo reikalavimų pažeidimus;** **3) duoda nurodymus kibernetinio saugumo subjektams nutraukti veiksmus, kurie pažeidžia šio įstatymo nustatytus reikalavimus, ir tokių veiksmų nebekartoti;** **4) duoda nurodymus kibernetinio saugumo subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų naudojamos kibernetinio saugumo rizikos valdymo priemonės atitiktų šio įstatymo 14 straipsnio 1 dalyje nurodytus teisės aktus arba kad jie įvykdytų šio įstatymo 18 straipsnio 1 dalyje nustatytą pareigą pranešti apie kibernetinius incidentus;**	Visiškas

g) prašyti pateikti kibernetinio saugumo politikos įgyvendinimo įrodymus, pavyzdžiui, kvalifikuoto auditoriaus atliktų saugumo auditų rezultatus ir atitinkamus pagrindinius įrodymus. Pirmos pastraipos b punkte nurodyti tiksliniai saugumo auditai grindžiami kompetentingos institucijos arba audituojamo subjekto atliktais rizikos vertinimais arba kita turima su rizika susijusia informacija. Bet kokio tikslinio saugumo audito rezultatai pateikiami kompetentingai institucijai. Tokio tikslinio saugumo audito, kurį atlieka nepriklausoma įstaiga, išlaidas padengia audituojamas subjektas, išskyrus tinkamai pagrįstus atvejus, kai kompetentinga institucija nusprendžia kitaip.	**5) duoda nurodymus kibernetinio saugumo subjektams informuoti fizinius arba juridinius asmenis, kuriems jie teikia paslaugas arba vykdo jiems aktualią veiklą ir kuriuos didelė kibernetinė grėsmė gali paveikti, apie grėsmės pobūdį, taip pat apie visus galimus veiksmus, kurių gali imtis tie fiziniai ar juridiniai asmenys, reaguodami į tą grėsmę;** **6) duoda nurodymus kibernetinio saugumo subjektams per pagrįstą terminą įgyvendinti kibernetinio saugumo audito metu pateiktas rekomendacijas;** **7) paskiria stebėsenos pareigūną, kuriam per nustatytą laikotarpį pavestos aiškiai apibrėžtos užduotys, prižiūrėti, kaip esminiai subjektai laikosi šio įstatymo 14 ir 18 straipsnių reikalavimų;** **8) duoda nurodymus kibernetinio saugumo subjektams konkrečiu būdu viešai paskelbti šio įstatymo pažeidimo aspektus;** **9) skiria kibernetinio saugumo subjektams baudą šio įstatymo 30 ir 31 straipsniuose nustatyta tvarka, kartu su bet kuriomis šios dalies 1–8, 10 ir 11 punktuose nurodytomis priemonėmis;** **10) inicijuoja šio įstatymo 32 straipsnyje nustatytą laikiną teisės užsiimti dalimi ar visa esminio subjekto vykdoma veikla ar teikti paslaugas sustabdymą;** **11) inicijuoja šio įstatymo 33 straipsnyje nustatytą esminio subjekto vadovo, išskyrus Lietuvos Respublikos Seimo, Vyriausybės ir Prezidento sprendimu skiriamus viešojo administravimo subjektų vadovus, laikiną nušalinimą nuo pareigų.** **<...>** **3. Taikydamas bet kurią iš šio straipsnio 1 dalyje nurodytų vykdymo užtikrinimo priemonių, Nacionalinis kibernetinio saugumo centras atsižvelgia į kiekvieno konkretaus atvejo aplinkybes, taip pat į:** **1) atsakomybę lengvinančias aplinkybes,, nustatytas šio straipsnio 4 dalyje, atsakomybę sunkinančias aplinkybės, nustatytas šio straipsnio 5 dalyje, ir pažeistų nuostatų pavojingumą, nurodytą šio įstatymo 29 straipsnyje;** **2) pažeidimo trukmę;** **3) subjekto įvykdytus ankstesnius šio įstatymo pažeidimus per pastaruosius 2 metus;** **4) padarytą turtinę arba neturtinę žalą, kuri vertinama apskaičiuojant finansinius ar ekonominius nuostolius, poveikį kitoms paslaugoms ir paveiktų naudotojų skaičių, nuostolių atlyginimą ar padaryto neigiamo poveikio panaikinimo;**	

	5) priemones, kurių subjektas ėmėsi siekdamas užkirsti kelią turtinei ar neturtinei žalai arba ją sumažinti; **6) patvirtintų elgesio kodeksų arba patvirtintų sertifikavimo mechanizmų laikymąsi;** **7) bendradarbiavimą su Nacionaliniu kibernetinio saugumo centru;** **8) pažeidimo mastą.** **4. Šio straipsnio 3 dalies 1 punkte nurodytomis atsakomybę lengvinančiomis aplinkybėmis laikoma:** **1) subjektas savo noru užkirto kelią turtinei ar neturtinei žalai;** **2) subjektas atlygino padarytą žalą;** **3) subjektas pripažino pažeidimą ir padėjo Nacionaliniam kibernetinio saugumo centrui patikrinimo metu;** **4) subjektas savo valia nutraukė pažeidimą;** **5) pažeidimas padarytas dėl neatsargumo;** **6) subjekto, kuris yra ūkio subjektas, finansinė padėtis yra labai sunki.** **5. Šio straipsnio 3 dalies 1 punkte nurodytomis atsakomybę sunkinančiomis aplinkybėmis laikoma:** **1) pažeidimas padarytas pakartotinai. Laikoma, kad pažeidimas padarytas pakartotinai, jeigu asmuo, įtariamas pažeidimo padarymu, per paskutinius 12 mėnesių nuo sprendimo, kuriuo buvo paskirta vykdymo užtikrinimo priemonė, įsigaliojimo dienos padarė tokį patį pažeidimą. Padarius pakartotinį pažeidimą, šioje dalyje nustatytas terminas skaičiuojamas iš naujo;** **2) padarytas pavojingas pažeidimas, kaip jis suprantamas pagal šio įstatymo 29 straipsnio 2 dalį;** **3) subjektas neištaisė trūkumų pagal Nacionalinio kibernetinio saugumo centro pateiktus nurodymus;** **4) subjektas trukdė vykdyti kibernetinio saugumo audito ar stebėsenos pareigūno veiklą, kurią įpareigojo atlikti Nacionalinis kibernetinio saugumo centras, nustatęs pažeidimą;** **5) subjektas pateikė neteisingą informaciją, susijusios su šio įstatymo reikalavimais;** **6) subjektas slėpė padarytą pažeidimą ar pažeidimą tęsė nepaisant to, kad Nacionalinis kibernetinio saugumo centras buvo atkreipęs dėmesį į pažeidimus ar veiklos trūkumus.** **7) pažeidimas padarytas tyčia.**	

	6. Šio straipsnio 1 dalyje nurodytos vykdymo užtikrinimo priemonės taikomos Vyriausybės nustatyta vykdymo užtikrinimo priemonių taikymo tvarka. **7. Sprendimas dėl vykdymo užtikrinimo priemonės skyrimo gali būti priimtas, jeigu praėjo ne daugiau kaip 2 metai nuo pažeidimo dienos (išskyrus atvejus, kai sprendimo dėl vykdymo užtikrinimo priemonės skyrimo metu pažeidimas ar trūkumas jau yra ištaisytas), o kai pažeidimas trunkamasis – nuo jo paaiškėjimo dienos.**	
3. Naudodamosi savo įgaliojimais pagal 2 dalies e, f arba g punktą, kompetentingos institucijos nurodo prašymo tikslą ir tiksliai apibrėžia prašomą informaciją.	**KSĮ projektas** **27 straipsnis. Bendrieji kibernetinio saugumo subjektų patikrinimų atlikimo pagrindai** <...> **3. Atlikdamas šio įstatymo 26 straipsnio 1 dalyje nurodytus patikrinimus, Nacionalinis kibernetinio saugumo centras turi teisę:** <...> **3) duoti nurodymus pateikti visą reikalingą informaciją, dokumentų kopijas ir išrašus, duomenų kopijas, taip pat susipažinti su visais duomenimis ir dokumentais, reikalingais kibernetinio saugumo subjektų tinklų ir informacinių sistemų atitikčiai šio įstatymo 14 straipsnio 1 dalyje nurodytiems reikalavimams įvertinti, įskaitant atliktų kibernetinio saugumo auditų rezultatus, įrodančius tinklų ir informacinių sistemų atitiktį nurodytiems reikalavimams;** <...> **5. Taikant šio straipsnio 3 dalies 3 punktą, Nacionalinis kibernetinio saugumo centras privalo nurodyti konkretų prašymo tikslą, pagrindą ir tiksliai apibrėžti prašomą informaciją.**	Visiškas
4. Valstybės narės užtikrina, kad jų kompetentingos institucijos, naudodamosi savo vykdymo užtikrinimo įgaliojimais esminių subjektų atžvilgiu, turėtų bent šiuos įgaliojimus: a) teikti įspėjimus, kad atitinkami subjektai pažeidžia šią direktyvą; b) priimti privalomus nurodymus, įskaitant nurodymus dėl priemonių, kurių reikia siekiant užkirsti kelią incidentui arba jam išspręsti, ir tokių priemonių įgyvendinimo bei ataskaitų apie jų įgyvendinimą terminus, arba įsakymą, kuriuo reikalaujama, kad atitinkami subjektai pašalintų nustatytus trūkumus arba ištaisytų šios direktyvos pažeidimus;	**KSĮ projektas** **28 straipsnis. Vykdymo užtikrinimo priemonės** **1. Nacionalinis kibernetinio saugumo centras, šio įstatymo 26 straipsnio 1 dalyje nurodyto patikrinimo metu nustatęs šio įstatymo pažeidimą, taiko vykdymo užtikrinimo priemonę ar jų grupę:** **1) teikia įspėjimus, kad kibernetinio saugumo subjektai pažeidžia šio įstatymo nustatytus reikalavimus;** **2) duoda nurodymus esminiams subjektams dėl priemonių, kurių reikia siekiant užkirsti kelią kibernetiniam incidentui arba jam suvaldyti, ir tokių priemonių įgyvendinimo bei jų įgyvendinimo ataskaitų pateikimo terminų, nurodymus kibernetinio saugumo subjektams, kad atitinkami subjektai**	Visiškas

c) nurodyti atitinkamiems subjektams nutraukti veiksmus, kurie pažeidžia šią direktyvą, ir tokių veiksmų nebekartoti; d) nurodyti atitinkamiems subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų kibernetinio saugumo rizikos valdymo priemonės atitiktų 21 straipsnį arba kad jie įvykdytų 23 straipsnyje nustatytas pareigas pranešti; e) įpareigoti atitinkamus subjektus informuoti fizinius arba juridinius asmenis, kuriems jie teikia paslaugas arba vykdo veiklą ir kuriuos didelė kibernetinė grėsmė gali paveikti, apie grėsmės pobūdį, taip pat apie visas galimas apsaugos ar taisomąsias priemones, kurių gali imtis tie fiziniai ar juridiniai asmenys, reaguodami į tą grėsmę; f) įpareigoti atitinkamus subjektus per pagrįstą terminą įgyvendinti saugumo audito metu pateiktas rekomendacijas; g) paskirti stebėsenos pareigūną, kuriam per nustatytą laikotarpį pavestos aiškiai apibrėžtos užduotys, prižiūrėti, kaip atitinkami subjektai laikosi 21 ir 23 straipsnių; h) įpareigoti atitinkamus subjektus konkrečiu būdu viešai paskelbti šios direktyvos pažeidimo aspektus; i) skirti arba prašyti, kad atitinkamos įstaigos ar teismai pagal nacionalinę teisę skirtų administracinę baudą pagal 34 straipsnį, kartu su bet kuriomis šios dalies a–h punktuose nurodytomis priemonėmis.	**pašalintų nustatytus trūkumus arba ištaisytų šio įstatymo reikalavimų pažeidimus;** **3) duoda nurodymus kibernetinio saugumo subjektams nutraukti veiksmus, kurie pažeidžia šio įstatymo nustatytus reikalavimus, ir tokių veiksmų nebekartoti;** **4) duoda nurodymus kibernetinio saugumo subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų naudojamos kibernetinio saugumo rizikos valdymo priemonės atitiktų šio įstatymo 14 straipsnio 1 dalyje nurodytus teisės aktus arba kad jie įvykdytų šio įstatymo 18 straipsnio 1 dalyje nustatytą pareigą pranešti apie kibernetinius incidentus;** **5) duoda nurodymus kibernetinio saugumo subjektams informuoti fizinius arba juridinius asmenis, kuriems jie teikia paslaugas arba vykdo jiems aktualią veiklą ir kuriuos didelė kibernetinė grėsmė gali paveikti, apie grėsmės pobūdį, taip pat apie visus galimus veiksmus, kurių gali imtis tie fiziniai ar juridiniai asmenys, reaguodami į tą grėsmę;** **6) duoda nurodymus kibernetinio saugumo subjektams per pagrįstą terminą įgyvendinti kibernetinio saugumo audito metu pateiktas rekomendacijas;** **7) paskiria stebėsenos pareigūną, kuriam per nustatytą laikotarpį pavestos aiškiai apibrėžtos užduotys, prižiūrėti, kaip esminiai subjektai laikosi šio įstatymo 14 ir 18 straipsnių reikalavimų;** **8) duoda nurodymus kibernetinio saugumo subjektams konkrečiu būdu viešai paskelbti šio įstatymo pažeidimo aspektus;** **9) skiria kibernetinio saugumo subjektams baudą šio įstatymo 30 ir 31 straipsniuose nustatyta tvarka, kartu su bet kuriomis šios dalies 1–8, 10 ir 11 punktuose nurodytomis priemonėmis;** **10) inicijuoja šio įstatymo 32 straipsnyje nustatytą laikiną teisės užsiimti dalimi ar visa esminio subjekto vykdoma veikla ar teikti paslaugas sustabdymą;** **11) inicijuoja šio įstatymo 33 straipsnyje nustatytą esminio subjekto vadovo, išskyrus Lietuvos Respublikos Seimo, Vyriausybės ir Prezidento sprendimu skiriamus viešojo administravimo subjektų vadovus, laikiną nušalinimą nuo pareigų.** **<...>** **3. Taikydamas bet kurią iš šio straipsnio 1 dalyje nurodytų vykdymo užtikrinimo priemonių, Nacionalinis kibernetinio saugumo centras atsižvelgia į kiekvieno konkretaus atvejo aplinkybes, taip pat į:**	

	1) atsakomybę lengvinančias aplinkybes, nustatytas šio straipsnio 4 dalyje, atsakomybę sunkinančias aplinkybės, nustatytas šio straipsnio 5 dalyje, ir pažeistų nuostatų pavojingumą, nurodytą šio įstatymo 29 straipsnyje; **2) pažeidimo trukmę;** **3) subjekto įvykdytus ankstesnius šio įstatymo pažeidimus per pastaruosius 2 metus;** **4) padarytą turtinę arba neturtinę žalą, kuri vertinama apskaičiuojant finansinius ar ekonominius nuostolius, poveikį kitoms paslaugoms ir paveiktų naudotojų skaičių, nuostolių atlyginimą ar padaryto neigiamo poveikio panaikinimo;** **5) priemones, kurių subjektas ėmėsi siekdamas užkirsti kelią turtinei ar neturtinei žalai arba ją sumažinti;** **6) patvirtintų elgesio kodeksų arba patvirtintų sertifikavimo mechanizmų laikymąsi;** **7) bendradarbiavimą su Nacionaliniu kibernetinio saugumo centru;** **8) pažeidimo mastą.** **4. Šio straipsnio 3 dalies 1 punkte nurodytomis atsakomybę lengvinančiomis aplinkybėmis laikoma:** **1) subjektas savo noru užkirto kelią turtinei ar neturtinei žalai;** **2) subjektas atlygino padarytą žalą;** **3) subjektas pripažino pažeidimą ir padėjo Nacionaliniam kibernetinio saugumo centrui patikrinimo metu;** **4) subjektas savo valia nutraukė pažeidimą;** **5) pažeidimas padarytas dėl neatsargumo;** **6) subjekto, kuris yra ūkio subjektas, finansinė padėtis yra labai sunki.** **5. Šio straipsnio 3 dalies 1 punkte nurodytomis atsakomybę sunkinančiomis aplinkybėmis laikoma:** **1) pažeidimas padarytas pakartotinai. Laikoma, kad pažeidimas padarytas pakartotinai, jeigu subjektas, įtariamas pažeidimo padarymu, per paskutinius 12 mėnesių nuo sprendimo, kuriuo buvo paskirta vykdymo užtikrinimo priemonė, įsigaliojimo dienos padarė tokį patį pažeidimą. Padarius pakartotinį pažeidimą, šioje dalyje nustatytas terminas skaičiuojamas iš naujo;** **2) padarytas pavojingas pažeidimas, kaip jis suprantamas pagal šio įstatymo 29 straipsnio 2 dalį;** **3) subjektas neištaisė trūkumų pagal Nacionalinio kibernetinio saugumo centro pateiktus nurodymus;**	

	4) subjektas trukdė vykdyti kibernetinio saugumo audito ar stebėsenos pareigūno veiklą, kurią įpareigojo atlikti Nacionalinis kibernetinio saugumo centras, nustatęs pažeidimą; **5) subjektas pateikė neteisingą informaciją, susijusios su šio įstatymo reikalavimais;** **6) subjektas slėpė padarytą pažeidimą ar pažeidimą tęsė nepaisant to, kad Nacionalinis kibernetinio saugumo centras buvo atkreipęs dėmesį į pažeidimus ar veiklos trūkumus;** **7) pažeidimas padarytas tyčia.** **6. Šio straipsnio 1 dalyje nurodytos vykdymo užtikrinimo priemonės taikomos Vyriausybės nustatyta vykdymo užtikrinimo priemonių taikymo tvarka.** **7. Sprendimas dėl vykdymo užtikrinimo priemonės skyrimo gali būti priimtas, jeigu praėjo ne daugiau kaip 2 metai nuo pažeidimo dienos (išskyrus atvejus, kai sprendimo dėl vykdymo užtikrinimo priemonės skyrimo metu pažeidimas ar trūkumas jau yra ištaisytas), o kai pažeidimas trunkamasis – nuo jo paaiškėjimo dienos.**	
5. Jei pagal 4 dalies a–d ir f punktus patvirtintos vykdymo užtikrinimo priemonės yra neveiksmingos, valstybės narės užtikrina, kad jų kompetentingos institucijos turėtų įgaliojimus nustatyti terminą, iki kurio esminis subjektas turi imtis būtinų veiksmų trūkumams pašalinti arba tų institucijų reikalavimams įvykdyti. Jei per nustatytą terminą nesiimama prašomų veiksmų, valstybės narės užtikrina, kad jų kompetentingos institucijos turėtų įgaliojimus: a) laikinai sustabdyti arba prašyti, kad sertifikavimo arba leidimus išduodanti įstaiga, arba teismas pagal nacionalinę teisę laikinai sustabdytų sertifikavimą arba įgaliojimą, susijusį su dalimi arba visomis esminio subjekto teikiamomis atitinkamomis paslaugomis ar vykdoma veikla; b) reikalauti, kad atitinkamos įstaigos arba teismai pagal nacionalinę teisę nustatytų laikiną draudimą bet kuriam esminiame subjekte generalinio direktoriaus ar teisinio atstovo lygmens vadovaujamas pareigas einančiam fiziniam asmeniui eiti vadovaujamas pareigas tame subjekte.	**KSĮ projektas** **28 straipsnis. Vykdymo užtikrinimo priemonės** **1. Nacionalinis kibernetinio saugumo centras, šio įstatymo 26 straipsnio 1 dalyje nurodyto patikrinimo metu nustatęs šio įstatymo pažeidimą, taiko vykdymo užtikrinimo priemonę ar jų grupę:** <...> **10) inicijuoja šio įstatymo 32 straipsnyje nustatytą laikiną teisės užsiimti dalimi ar visa esminio subjekto vykdoma veikla ar teikti paslaugas sustabdymą;** **11) inicijuoja šio įstatymo 33 straipsnyje nustatytą esminio subjekto vadovo, išskyrus Lietuvos Respublikos Seimo, Vyriausybės ir Prezidento sprendimu skiriamus viešojo administravimo subjektų vadovus, laikiną nušalinimą nuo pareigų.** **32 straipsnis. Laikinas teisės užsiimti dalimi ar visa esminio subjekto vykdoma veikla ar teikti paslaugas sustabdymas** **1. Teismas, gavęs Nacionalinio kibernetinio saugumo centro prašymą, nutartimi turi teisę laikinai sustabdyti teisę užsiimti dalimi ar visa esminio subjekto vykdoma veikla, jeigu nustatoma, kad šio įstatymo 28 straipsnio 1 dalies**	Visiškas

Laikini sustabdymai arba draudimai, nustatyti pagal šią dalį, taikomi tik tol, kol atitinkamas subjektas nesiims būtinų veiksmų trūkumams pašalinti arba kompetentingos institucijos reikalavimams, dėl kurių taikytos tokios vykdymo užtikrinimo priemonės, įvykdyti. Skiriant tokius laikinus sustabdymus ar draudimus, turi būti taikomos tinkamos procedūrinės apsaugos priemonės pagal bendruosius Sąjungos teisės ir Chartijos principus, įskaitant teisę į veiksmingą teisinę gynybą bei teisingą bylos nagrinėjimą, nekaltumo prezumpciją ir teisę į gynybą. Šioje dalyje numatytos vykdymo užtikrinimo priemonės netaikomos viešojo administravimo subjektams, kuriems taikoma ši direktyva.	**1–4 ir 6 punktuose numatytų vykdymo užtikrinimo priemonių taikymas yra neveiksmingas.** **2. Nacionalinis kibernetinio saugumo centras, prieš kreipdamasis į teismą su prašymu laikinai sustabdyti teisę užsiimti dalimi ar visa esminio subjekto vykdoma veikla šio straipsnio 1 dalyje nurodytu pagrindu, privalo esminį subjektą informuoti pateikdamas esminę informaciją apie teisės aktų nuostatas ir nustatytus faktinius duomenis, kurie sudaro laikino teisės užsiimti dalimi ar visa esminio subjekto vykdoma veikla sustabdymo pagrindus, ir nustatyti terminą, kuris negali būti trumpesnis kaip 10 darbo dienų nuo pranešimo įteikimo dienos, iki kurio esminis subjektas turi imtis būtinų veiksmų nustatytiems trūkumams pašalinti ar reikalavimams įvykdyti. Nacionalinis kibernetinio saugumo centras šio straipsnio 1 dalyje nustatytu pagrindu į teismą turi teisę kreiptis tik pasibaigus Nacionalinis kibernetinio saugumo centro nustatytam terminui ir esminiam subjektui nesiėmus nurodytų veiksmų.** **3. Nacionalinio kibernetinio saugumo centro prašyme teismui dėl teisės laikinai sustabdyti teisę užsiimti dalimi ar visa esminio subjekto vykdoma veikla turi būti nurodyta:** **1) esminio subjekto vykdoma veikla ar jos dalis ar teikiamos paslaugos, kurias prašoma stabdyti;** **2) aplinkybės, įrodančios, kad šio įstatymo 28 straipsnio 1 dalies 1–4 ir 6 punktuose numatytų užtikrinimo priemonių taikymas yra neveiksmingas;** **3) aplinkybės, įrodančios, kad esminiam subjektui buvo nustatytas terminas trūkumams pašalinti ar reikalavimams įvykdyti, o esminis subjektas nesiėmė nurodytų veiksmų;** **4) esminio subjekto, kurio teisę užsiimti dalimi ar visa vykdoma veikla ar teikti paslaugas prašoma stabdyti, paaiškinimai, jeigu tokie buvo gauti.** **4. Nutartyje laikinai sustabdyti teisę užsiimti dalimi ar visa esminio subjekto vykdoma veikla juridinis asmuo įpareigojamas laikinai nutraukti visą steigimo dokumentuose numatytą ūkinę, komercinę, finansinę, profesinę veiklą ar jos dalį ir uždaryti visus šia veikla ar jos dalimi susijusius padalinius. Nutartyje nurodomas laikino juridinio asmens veiklos sustabdymo terminas, kuris negali būti ilgesnis kaip 4 mėnesiai. Jeigu aplinkybės, kad šio įstatymo 28 straipsnio 1 dalies 1–4 ir 6 punktuose numatytų užtikrinimo priemonių taikymas yra neveiksmingas, išlieka, gavus Nacionalinio kibernetinio saugumo centro prašymą, teismo nutartimi šis terminas gali būti pratęstas, bet ne ilgiau kaip 2 mėnesiams. Pratęsimu skaičius neribojamas.**	

	5. Nutartis, kuria laikinai sustabdoma dalis ar visa juridinio asmens veikla, nedelsiant nusiunčiama asmeniui, prašiusiam taikyti dalies ar visos juridinio asmens veiklos sustabdymą. **6. Nutartis esminiam subjektui ar jo atstovui paskelbiama Civilinio proceso kodekso nustatyta tvarka.** **7. Esminis subjektas teismo nutartį laikinai sustabdyti esminio subjekto veiklą gali apskųsti aukštesnės instancijos teismui per 5 darbo dienas nuo nutarties gavimo dienos.** **8. Teismas privalo panaikinti juridinio asmens veiklos laikiną sustabdymą, kai Nacionalinis kibernetinio saugumo centras prašo panaikinti laikiną sustabdymą. Nacionalinis kibernetinio saugumo centras, nustatęs, kad juridinio asmens veiklos laikinas sustabdymas yra nebereikalingas, ne vėliau kaip per 5 darbo dienas nuo šių aplinkybių paaiškėjimo, privalo prašyti teismo panaikinti laikiną sustabdymą** **9. Nacionalinis kibernetinio saugumo centras informaciją apie subjektą, kuriam laikinai sustabdyta teisė užsiimti dalimi ar visa juridinio asmens vykdoma veikla ar teikti paslaugas, skelbia savo interneto svetainėje.** **33 straipsnis. Esminio subjekto vadovo laikinas nušalinimas nuo pareigų** **1. Teismas, gavęs Nacionalinio kibernetinio saugumo centro prašymą laikinai nušalinti esminio subjekto vadovą nuo pareigų, nutartimi turi teisę laikinai nušalinti esminio subjekto vadovą nuo pareigų, jeigu nustatoma, kad šio įstatymo 28 straipsnio 1 dalies 1–4 ir 6 punktuose numatytų vykdymo užtikrinimo priemonių taikymas yra neveiksmingas.** **2. Nacionalinis kibernetinio saugumo centras, prieš kreipdamasis į teismą su prašymu laikinai nušalinti esminio subjekto vadovą nuo pareigų šio straipsnio 1 dalyje nurodytu pagrindu, privalo esminį subjektą informuoti pateikdamas esminę informaciją apie teisės aktų nuostatas ir nustatytus faktinius duomenis, kurie sudaro laikino esminio subjekto vadovo nušalinimo nuo pareigų pagrindus, ir nustatyti terminą, kuris negali būti trumpesnis kaip 10 darbo dienų nuo pranešimo įteikimo dienos, per kurį esminis subjektas turi imtis būtinų veiksmų nustatytiems trūkumams pašalinti ar reikalavimams įvykdyti. Nacionalinis kibernetinio saugumo centras šio straipsnio 1 dalyje nustatytu pagrindu į teismą turi teisę kreiptis tik pasibaigus Nacionalinis kibernetinio saugumo centro nustatytam terminui ir esminiam subjektui nesiėmus nurodytų veiksmų.**	

	3. Nacionalinio kibernetinio saugumo centro prašyme teismui dėl esminio subjekto vadovo laikino nušalinimo nuo pareigų turi būti nurodyta: **1) aplinkybės, įrodančios, kad šio įstatymo 28 straipsnio 1 dalies 1–4 ir 6 punktuose numatytų užtikrinimo priemonių taikymas yra neveiksmingas;** **2) aplinkybės, įrodančios, kad esminiam subjektui buvo nustatytas terminas trūkumams pašalinti ar reikalavimams įvykdyti, o esminis subjektas nesiėmė nurodytų veiksmų;** **3) esminio subjekto, kurio vadovą prašoma laikinai nušalinti nuo pareigų, paaiškinimai, jeigu tokie buvo gauti.** **4. Nutartis, kuria esminio subjekto vadovas laikinai nušalinimas nuo pareigų, nedelsiant nusiunčiama jį į pareigas priimančiam subjektui.** **5. Nutartis esminio subjekto vadovui ar jo atstovui paskelbiama Civilinio proceso kodekso nustatyta tvarka.** **6. Nuo teismo nutarties laikinai nušalinti esminio subjekto vadovą nuo pareigų paskelbimo dienos nušalintas nuo pareigų fizinis asmuo neturi teisės atlikti savo funkcijų ir visi po tokio teismo sprendimo paskelbimo dienos jo priimti sprendimai yra negaliojantys.** **7. Laikinas esminio subjekto vadovo nušalinimas nuo pareigų negali trukti ilgiau kaip šešis mėnesius. Prireikus šios priemonės taikymas gali būti pratęstas dar iki trijų mėnesių. Pratęsimų skaičius neribojamas, bet visais atvejais nušalinimas nuo pareigų negali trukti ilgiau nei to reikia, kad būtų užtikrinamas šio įstatymo nuostatų laikymasis** **8. Nutartį laikinai nušalinti esminio subjekto vadovą nuo pareigų, taip pat nutartį pratęsti šios priemonės taikymo terminą per 5 darbo dienas nuo nutarties paskelbimo esminis subjektas ar nušalintas esminio subjekto vadovas gali apskųsti aukštesnės instancijos teismui. Šio teismo priimta nutartis yra galutinė ir neskundžiama.** **9. Teismas privalo panaikinti laikiną esminio subjekto vadovo nušalinimą nuo pareigų ar laikiną teisės užsiimti tam tikra veikla sustabdymą, kai Nacionalinis kibernetinio saugumo centras prašo panaikinti laikiną sustabdymą. Nacionalinis kibernetinio saugumo centras, gavęs motyvuotą nušalinto esminio subjekto vadovo prašymą ir nustatęs, kad esminio subjekto vadovo nušalinimas yra nebereikalingas, ne vėliau kaip per 7 darbo dienas nuo prašymo gavimo dienos, privalo prašyti teismo panaikinti laikiną sustabdymą**	

	10. Nacionalinis kibernetinio saugumo centras informaciją apie esminį subjektą, kurio vadovas laikinai nušalintas nuo pareigų, skelbia savo interneto svetainėje.	
6. Valstybės narės užtikrina, kad fizinis asmuo, atsakingas už esminį subjektą arba veikiantis kaip jo teisinis atstovas, remdamasis jam suteiktais įgaliojimais atstovauti tam subjektui, įgaliojimu priimti sprendimus jo vardu arba įgaliojimu vykdyti jo kontrolę, turėtų įgaliojimus užtikrinti, kad subjektas laikytųsi šios direktyvos. Valstybės narės užtikrina, kad tie fiziniai asmenys galėtų būti traukiami atsakomybėn už jų pareigų užtikrinti šios direktyvos laikymąsi. Viešojo administravimo subjektų atžvilgiu šia dalimi nedaromas poveikis nacionalinės teisės aktams, susijusiems su valstybės tarnautojų ir renkamų ar paskirtų pareigūnų atsakomybe.	**KSĮ projektas** **14 straipsnis. Kibernetinio saugumo rizikos valdymo priemonės** **<...>** **6. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo privalo užtikrinti, kad kibernetinio saugumo subjektas laikytųsi šiame įstatyme jam nustatytų pareigų, ir prižiūrėti jų laikymąsi. Kibernetinio saugumo subjekto vadovas, įgaliodamas šioje dalyje nurodytą asmenį, užtikrina, kad jis turėtų būtinų priemonių, reikalingų nurodytam įgaliojimui vykdyti.** **15 straipsnis. Už kibernetinį saugumą atsakingi asmenys** **1. Kibernetinio saugumo subjekto vadovas ar jo įgaliotas asmuo privalo paskirti kibernetinio saugumo vadovą, tiesiogiai atskaitingą kibernetinio saugumo subjekto vadovui, atsakingą už atitikties šio įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantį kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas.** **2. Kibernetinio saugumo subjekto vadovas ar jo įgaliotas asmuo privalo paskirti saugos įgaliotinį, atsakingą už konkrečios tinklų ir informacinės sistemos atitiktį šio įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams ir atliekantį kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas.** **3. Kibernetinio saugumo vadovas gali vykdyti saugos įgaliotinio funkcijas. Kibernetinio saugumo vadovas gali būti paskirtas atsakingas už šio įstatymo 14 ir 18 straipsniuose nustatytų reikalavimų, taikomų keliems kibernetinio saugumo subjektams, gyvendinimą. Saugos įgaliotinis gali būti paskirtas atsakingas už kelių tinklų ir informacinių sistemų atitiktį šio įstatymo 14 straipsnyje nustatytiems reikalavimams. Sprendimą dėl šioje dalyje numatytų už kibernetinį saugumą atsakingų asmenų skyrimo priima kibernetinio saugumo subjekto vadovas, atsižvelgdamas į kibernetinio saugumo subjekto organizacinę struktūrą ir dydį.** **ANK projektas**	Visiškas

	„480 straipsnis. Lietuvos Respublikos kibernetinio saugumo įstatyme nustatytų kibernetinio saugumo užtikrinimo pareigų atlikimo pažeidimai **<...>** **3. Lietuvos Respublikos kibernetinio saugumo įstatyme nustatytų reikalavimų kibernetinio saugumo subjektų vadovams ar jų įgaliotiems asmenims pažeidimas** **užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar jų įgaliotiems asmenims nuo dviejų šimtų penkiasdešimt iki trijų tūkstančių eurų.** **4. Šio straipsnio 3 dalyje numatytas administracinis nusižengimas, padarytas pakartotinai,** **užtraukia baudą nuo dviejų tūkstančių iki šešių tūkstančių eurų.“**	
7. Imdamosi bet kurios iš 4 dalyje nurodytų vykdymo užtikrinimo priemonių kompetentingos institucijos gerbia teisę į gynybą ir atsižvelgia į kiekvieno konkretaus atvejo aplinkybes ir tinkamai atsižvelgia bent į: a) pažeidimo sunkumą ir pažeistų nuostatų svarbą; sunkiais pažeidimais, inter alia, bet kuriuo atveju laikomi: i) pakartotiniai pažeidimai; ii) nepranešimas apie didelius incidentus; iii) trūkumų pagal kompetentingų institucijų privalomus vykdyti nurodymus neištaisymas; iv) trukdymas vykdyti audito ar stebėsenos veiklą, kurią įpareigojo atlikti kompetentinga institucija nustačius pažeidimą; v) neteisingos ar labai netikslios informacijos, susijusios su kibernetinio saugumo rizikos valdymo priemonėmis arba pareigomis pranešti, nustatytomis 21 ir 23 straipsniuose, pateikimas; b) pažeidimo trukmę; c) atitinkamo subjekto įvykdytus svarbius ankstesnius pažeidimus; d) padarytą turtinę arba neturtinę žalą, įskaitant finansinius ar ekonominius nuostolius, poveikį kitoms paslaugoms ir paveiktų naudotojų skaičių; e) tai, ar pažeidimą įvykdęs asmuo veikė tyčia ar dėl neatsargumo;	**KSĮ projektas** **28 straipsnis. Vykdymo užtikrinimo priemonės** **<...>** **3. Taikydamas bet kurią iš šio straipsnio 1 dalyje nurodytų vykdymo užtikrinimo priemonių, Nacionalinis kibernetinio saugumo centras atsižvelgia į kiekvieno konkretaus atvejo aplinkybes, taip pat į:** **1) atsakomybę lengvinančias aplinkybes, nustatytas šio straipsnio 4 dalyje, atsakomybę sunkinančias aplinkybės, nustatytas šio straipsnio 5 dalyje, ir pažeistų nuostatų pavojingumą, nurodytą šio įstatymo 29 straipsnyje;** **2) pažeidimo trukmę;** **3) subjekto įvykdytus ankstesnius šio įstatymo pažeidimus per pastaruosius 2 metus;** **4) padarytą turtinę arba neturtinę žalą, kuri vertinama apskaičiuojant finansinius ar ekonominius nuostolius, poveikį kitoms paslaugoms ir paveiktų naudotojų skaičių, nuostolių atlyginimą ar padaryto neigiamo poveikio panaikinimo;** **5) priemones, kurių subjektas ėmėsi siekdamas užkirsti kelią turtinei ar neturtinei žalai arba ją sumažinti;** **6) patvirtintų elgesio kodeksų arba patvirtintų sertifikavimo mechanizmų laikymąsi;** **7) bendradarbiavimą su Nacionaliniu kibernetinio saugumo centru;** **8) pažeidimo mastą.** **4. Šio straipsnio 3 dalies 1 punkte nurodytomis atsakomybę lengvinančiomis aplinkybėmis laikoma:**	Visiškas

f) priemones, kurių subjektas ėmėsi siekdamas užkirsti kelią turtinei ar neturtinei žalai arba ją sumažinti; g) patvirtintų elgesio kodeksų arba patvirtintų sertifikavimo mechanizmų laikymąsi; h) atsakingais laikomų fizinių ar juridinių asmenų bendradarbiavimo su kompetentingomis institucijomis lygį.	**1) subjektas savo noru užkirto kelią turtinei ar neturtinei žalai;** **2) subjektas atlygino padarytą žalą;** **3) subjektas pripažino pažeidimą ir padėjo Nacionaliniam kibernetinio saugumo centrui patikrinimo metu;** **4) subjektas savo valia nutraukė pažeidimą;** **5) pažeidimas padarytas dėl neatsargumo;** **6) subjekto, kuris yra ūkio subjektas, finansinė padėtis yra labai sunki.** **5. Šio straipsnio 3 dalies 1 punkte nurodytomis atsakomybę sunkinančiomis aplinkybėmis laikoma:** **1) pažeidimas padarytas pakartotinai. Laikoma, kad pažeidimas padarytas pakartotinai, jeigu asmuo, įtariamas pažeidimo padarymu, per paskutinius 12 mėnesių nuo sprendimo, kuriuo buvo paskirta vykdymo užtikrinimo priemonė, įsigaliojimo dienos padarė tokį patį pažeidimą. Padarius pakartotinį pažeidimą, šioje dalyje nustatytas terminas skaičiuojamas iš naujo;** **2) padarytas pavojingas pažeidimas, kaip jis suprantamas pagal šio įstatymo 29 straipsnio 2 dalį;** **3) subjektas neištaisė trūkumų pagal Nacionalinio kibernetinio saugumo centro pateiktus nurodymus;** **4) subjektas trukdė vykdyti kibernetinio saugumo audito ar stebėsenos pareigūno veiklą, kurią įpareigojo atlikti Nacionalinis kibernetinio saugumo centras, nustatęs pažeidimą;** **5) subjektas pateikė neteisingą informaciją, susijusios su šio įstatymo reikalavimais;** **6) subjektas slėpė padarytą pažeidimą ar pažeidimą tęsė nepaisant to, kad Nacionalinis kibernetinio saugumo centras buvo atkreipęs dėmesį į pažeidimus ar veiklos trūkumus;** 7) pažeidimas padarytas tyčia.	
8. Kompetentingos institucijos išsamiai pagrindžia savo vykdymo užtikrinimo priemones. Prieš priimdamos tokias priemones kompetentingos institucijos atitinkamiems subjektams praneša apie savo preliminarias išvadas. Jos taip pat suteikia tiems subjektams pagrįstą laikotarpį pastaboms pateikti, išskyrus tinkamai pagrįstus atvejus, kai tai trukdytų imtis neatidėliotinų incidentų prevencijos arba reagavimo į juos veiksmų.	**KSĮ projektas** **27 straipsnis. Bendrieji kibernetinio saugumo subjektų patikrinimų atlikimo pagrindai** <...> **8. Prieš priimdamas sprendimą taikyti šio įstatymo 28 straipsnio 1 dalyje nurodytą vykdymo užtikrinimo priemonę (priemones), Nacionalinis kibernetinio saugumo centras privalo apie tai informuoti kibernetinio saugumo subjektą, kuriam ketinama taikyti vykdymo užtikrinimo priemonę (priemones),**	Visiškas

	pateikdamas esminę informaciją apie teisės aktų nuostatas ir nustatytus faktinius duomenis, kurie sudaro vykdymo užtikrinimo priemonės (priemonių) taikymo pagrindus, ir nustatyti ne trumpesnį kaip 20 darbo dienų terminą nuo pranešimo įteikimo dienos paaiškinimams pateikti, išskyrus atvejus, kai tai trukdytų imtis neatidėliotinų kibernetinių incidentų prevencijos arba reagavimo į juos veiksmų.	
9. Valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą informuotų toje pačioje valstybėje narėje esančias atitinkamas kompetentingas institucijas pagal Direktyvą (ES) 2022/2557, kai jos naudojasi savo priežiūros ir vykdymo užtikrinimo įgaliojimais, kuriais siekiama užtikrinti, kad subjektas, kuris pagal Direktyvą (ES) 2022/2557 identifikuotas kaip ypatingos svarbos subjektas, laikytųsi šios direktyvos. Kai taikytina, kompetentingos institucijos pagal Direktyvą (ES) 2022/2557 gali prašyti kompetentingų institucijų pagal šią direktyvą naudotis savo priežiūros ir vykdymo užtikrinimo įgaliojimais subjekto, kuris identifikuojamas kaip ypatingos svarbos subjektas pagal Direktyvą (ES) 2022/2557, atžvilgiu.	**KSĮ projektas** **20 straipsnis. Tarpinstitucinis bendradarbiavimas** **<...>** **2. Nacionalinis kibernetinio saugumo centras:** **1) ne vėliau kaip per 20 darbo dienų nuo sprendimo taikyti šio įstatymo 28 straipsnio 1 dalyje nurodytą vykdymo užtikrinimo priemonę priėmimo apie tai informuoja kompetentingą instituciją pagal Krizių valdymo ir civilinės saugos įstatymą, jeigu vykdymo užtikrinimo priemonė taikoma siekiant užtikrinti, kad esminis subjektas laikytųsi šio įstatymo reikalavimų.**	Visiškas
10. Valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą bendradarbiautų su atitinkamomis atitinkamos valstybės narės kompetentingomis institucijomis pagal Reglamentą (ES) 2022/2554. Visų pirma valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą informuotų Priežiūros forumą, įsteigtą pagal Reglamento (ES) 2022/2554 32 straipsnio 1 dalį, kai jos naudojasi priežiūros ir vykdymo užtikrinimo įgaliojimais, kuriais siekiama užtikrinti, kad esminis subjektas, paskirtas ypatingai svarbiu trečiųjų šalių IRT paslaugų teikėju pagal Reglamento (ES) 2022/2554 31 straipsnį, laikytųsi šios direktyvos.	**KSĮ projektas** **20 straipsnis. Tarpinstitucinis bendradarbiavimas** **<...>** **2. Nacionalinis kibernetinio saugumo centras:** **<...>** **2) ne vėliau kaip per 20 darbo dienų nuo sprendimo taikyti šio įstatymo 28 straipsnio 1 dalyje vykdymo užtikrinimo priemonę priėmimo apie tai informuoja kompetentingą instituciją pagal Reglamentą (ES) 2022/2554, jeigu vykdymo užtikrinimo priemonė taikoma siekiant užtikrinti, kad esminis subjektas, kuris paskirtas ypatingai svarbiu trečiųjų šalių informacinių ir ryšių technologijų paslaugų teikėju pagal Reglamento (ES) 2022/2554 31 straipsnį, laikytųsi šio įstatymo reikalavimų.**	Visiškas
33 straipsnis. Svarbių subjektų priežiūros ir jų pareigų vykdymo užtikrinimo priemonės		
1. Gavusios įrodymų, duomenų ar informacijos, kad svarbus subjektas, kaip įtariama, nesilaiko šios direktyvos, visų pirma jos 21 ir 23 straipsnių, valstybės narės užtikrina, kad kompetentingos institucijos prireikus imtųsi veiksmų taikydamos ex post	**KSĮ projektas** **26 straipsnis. Kibernetinio saugumo subjektų patikrinimai**	Visiškas

priežiūros priemones. Valstybės narės užtikrina, kad tos priemonės būtų veiksmingos, proporcingos ir atgrasomos, atsižvelgiant į kiekvieno konkretaus atvejo aplinkybes.	**1. Nacionalinis kibernetinio saugumo centras atlieka kibernetinio saugumo subjektų atitikties šio įstatymo reikalavimams, išskyrus nustatytus šio įstatymo VI ir VII skyriuose, patikrinimus.** **2. Nacionalinis kibernetinio saugumo centras turi teisę pradėti šio straipsnio 1 dalyje nurodytą kibernetinio saugumo subjekto patikrinimą bet kokiu klausimu, susijusiu su šio įstatymo reikalavimais, nustatytais kibernetinio saugumo subjektams, kurių nevykdymas laikomas pažeidimu, savo iniciatyva, gavęs skundą ar kitų šaltinių pagrindu, išskyrus šio straipsnio 3 dalyje nurodytus atvejus.** **3. Šio straipsnio 1 dalyje nurodyti svarbių subjektų patikrinimai atliekami tik gavus duomenų ar informacijos, kad svarbus subjektas, kaip įtariama, padarė šio įstatymo reikalavimų pažeidimą.** **27 straipsnis. Bendrieji kibernetinio saugumo subjektų patikrinimų atlikimo pagrindai** **<...>** **3. Atlikdamas šio įstatymo 26 straipsnio 1 dalyje nurodytus patikrinimus, Nacionalinis kibernetinio saugumo centras turi teisę:** **1) įeiti į tikrinamų kibernetinio saugumo subjektų patalpas (tarp jų ir nuomojamas ar naudojamas kitais pagrindais), ne ilgesniam kaip 30 kalendorinių dienų terminui, paimti dokumentų kopijas ir nuorašus, duomenų kopijas bei kitus daiktus, reikalingus patikrinimams atlikti. Įeiti į juridinio asmens patalpas (tarp jų ir nuomojamas ar naudojamas kitais pagrindais) galima tik juridinio asmens darbo laiku, pateikus tarnybinį pažymėjimą ir Nacionalinio kibernetinio saugumo centro sprendimą atlikti patikrinimą liudijantį dokumentą ar kitą Nacionalinio kibernetinio saugumo centro vadovo suteiktą įgaliojimą. Įeiti į fiziniam asmeniui priklausančias patalpas (tarp jų ir nuomojamas ar naudojamas kitais pagrindais) galima tik pateikus teismo nutartį dėl leidimo įeiti į fiziniam asmeniui priklausančias patalpas;** **2) duoti nurodymus tikrinamiems kibernetinio saugumo subjektams savo lėšomis atlikti nepriklausomą tinklų ir informacinių sistemų arba jomis vykdomos veiklos ar teikiamų paslaugų tikslinį kibernetinio saugumo auditą ir pateikti šio audito rezultatus, jeigu remiantis kibernetinio saugumo rizikos analizės rezultatais nustatytas aukštas rizikos lygis;** **3) duoti nurodymus pateikti visą reikalingą informaciją, dokumentų kopijas ir išrašus, duomenų kopijas, taip pat susipažinti su visais duomenimis ir**	

	dokumentais, reikalingais kibernetinio saugumo subjektų tinklų ir informacinių sistemų atitikčiai šio įstatymo 14 straipsnio 1 dalyje nurodytiems reikalavimams įvertinti, įskaitant atliktų kibernetinio saugumo auditų rezultatus, įrodančius tinklų ir informacinių sistemų atitiktį nurodytiems reikalavimams; **4) duoti nurodymus asmenims, turintiems patikrinimams reikšmingos informacijos, pateikti žodinius ir rašytinius paaiškinimus, reikalauti, kad jie atvyktų į Nacionalinio kibernetinio saugumo centro patalpas duoti paaiškinimų;** **5) savo lėšomis pasitelkti nepriklausomus, nešališkus, ir atitinkančius Valstybės tarnybos įstatyme nustatytus nepriekaištingos reputacijos kriterijus bei atitinkančią kvalifikaciją ir patirtį turinčius asmenis;** **6) sudaryti sutartis su audito įmonėmis, kitais juridiniais ar fiziniais asmenimis, kurių paslaugomis Nacionalinis kibernetinio saugumo centras naudosis atlikdamas patikrinimą. Sudarant šiame punkte nurodytas sutartis taikomi šio įstatymo 7 straipsnio 3 dalyje nurodyti reikalavimai;** **7) naudoti visą Nacionalinio kibernetinio saugumo centro turimą informaciją, įskaitant ir informaciją, gautą kitų patikrinimų metu;** **8) naudotis kitomis įstatymų suteiktomis teisėmis.** **4. Nacionaliniame kibernetinio saugumo centre einantys pareigas asmenys, užtikrindami jiems pavestų uždavinių ir funkcijų vykdymą atliekant patikrinimus, turi teises, kurias įgyvendina Nacionalinio kibernetinio saugumo centro vardu:** **1) atlikti veiksmus, nurodytus šio straipsnio 3 dalies 1 punkte;** **2) užfiksuoti faktines aplinkybes;** **3) patikrinimo metu savo lėšomis naudoti technines priemones;** **4) tikrinti asmenų tapatybę patvirtinančius dokumentus.**	
2. Valstybės narės užtikrina, kad kompetentingos institucijos, vykdydamos savo priežiūros užduotis, susijusias su svarbiais subjektais, turėtų bent šiuos įgaliojimus taikyti tiems subjektams: a) atlikti patikrinimus vietoje ir vykdyti ex post priežiūrą ne vietoje, kuriuos atlieka apmokyti specialistai; b) atlikti tikslinius saugumo auditus, kuriuos vykdo kvalifikuota nepriklausoma įstaiga arba kompetentinga institucija; c) atlikti saugumo patikrinimus, pagrįstus objektyviais, nediskriminaciniais, sąžiningais ir skaidriais rizikos vertinimo kriterijais, bendradarbiaudamos, kai to reikia, su atitinkamu subjektu;	**KSĮ projektas** **28 straipsnis. Vykdymo užtikrinimo priemonės** **1. Nacionalinis kibernetinio saugumo centras, šio įstatymo 26 straipsnio 1 dalyje nurodyto patikrinimo metu nustatęs šio įstatymo pažeidimą, taiko vykdymo užtikrinimo priemonę ar jų grupę:** **1) teikia įspėjimus, kad kibernetinio saugumo subjektai pažeidžia šio įstatymo nustatytus reikalavimus;** **2) duoda nurodymus esminiams subjektams dėl priemonių, kurių reikia siekiant užkirsti kelią kibernetiniam incidentui arba jam suvaldyti, ir tokių priemonių įgyvendinimo bei jų įgyvendinimo ataskaitų pateikimo terminų, nurodymus kibernetinio saugumo subjektams, kad atitinkami subjektai**	Visiškas

d) prašyti pateikti informaciją, būtiną atitinkamo subjekto priimtoms kibernetinio saugumo rizikos valdymo priemonėms įvertinti ex post, įskaitant dokumentais pagrįstą kibernetinio saugumo politiką, taip pat pareigos teikti informaciją kompetentingoms institucijoms pagal 28 straipsnį laikymąsi; e) prašyti leisti susipažinti su duomenimis, dokumentais ir informacija, reikalinga priežiūros užduotims atlikti; f) prašyti pateikti kibernetinio saugumo politikos įgyvendinimo įrodymus, pavyzdžiui, kvalifikuoto auditoriaus atliktų saugumo auditų rezultatus ir atitinkamus pagrindinius įrodymus. Pirmos pastraipos b punkte nurodyti tiksliniai saugumo auditai grindžiami kompetentingos institucijos arba audituojamo subjekto atliktais rizikos vertinimais arba kita turima su rizika susijusia informacija. Bet kokio tikslinio saugumo audito rezultatai pateikiami kompetentingai institucijai. Tokio tikslinio saugumo audito, kurį atlieka nepriklausoma įstaiga, išlaidas padengia audituojamas subjektas, išskyrus tinkamai pagrįstus atvejus, kai kompetentinga institucija nusprendžia kitaip.	**pašalintų nustatytus trūkumus arba ištaisytų šio įstatymo reikalavimų pažeidimus;** **3) duoda nurodymus kibernetinio saugumo subjektams nutraukti veiksmus, kurie pažeidžia šio įstatymo nustatytus reikalavimus, ir tokių veiksmų nebekartoti;** **4) duoda nurodymus kibernetinio saugumo subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų naudojamos kibernetinio saugumo rizikos valdymo priemonės atitiktų šio įstatymo 14 straipsnio 1 dalyje nurodytus teisės aktus arba kad jie įvykdytų šio įstatymo 18 straipsnio 1 dalyje nustatytą pareigą pranešti apie kibernetinius incidentus;** **5) duoda nurodymus kibernetinio saugumo subjektams informuoti fizinius arba juridinius asmenis, kuriems jie teikia paslaugas arba vykdo jiems aktualią veiklą ir kuriuos didelė kibernetinė grėsmė gali paveikti, apie grėsmės pobūdį, taip pat apie visus galimus veiksmus, kurių gali imtis tie fiziniai ar juridiniai asmenys, reaguodami į tą grėsmę;** **6) duoda nurodymus kibernetinio saugumo subjektams per pagrįstą terminą įgyvendinti kibernetinio saugumo audito metu pateiktas rekomendacijas;** **7) paskiria stebėsenos pareigūną, kuriam per nustatytą laikotarpį pavestos aiškiai apibrėžtos užduotys, prižiūrėti, kaip esminiai subjektai laikosi šio įstatymo 14 ir 18 straipsnių reikalavimų;** **8) duoda nurodymus kibernetinio saugumo subjektams konkrečiu būdu viešai paskelbti šio įstatymo pažeidimo aspektus;** **9) skiria kibernetinio saugumo subjektams baudą šio įstatymo 30 ir 31 straipsniuose nustatyta tvarka, kartu su bet kuriomis šios dalies 1–8, 10 ir 11 punktuose nurodytomis priemonėmis;** **10) inicijuoja šio įstatymo 32 straipsnyje nustatytą laikiną teisės užsiimti dalimi ar visa esminio subjekto vykdoma veikla ar teikti paslaugas sustabdymą;** **11) inicijuoja šio įstatymo 33 straipsnyje nustatytą esminio subjekto vadovo, išskyrus Lietuvos Respublikos Seimo, Vyriausybės ir Prezidento sprendimu skiriamus viešojo administravimo subjektų vadovus, laikiną nušalinimą nuo pareigų.**	
3. Naudodamosi savo įgaliojimais pagal 2 dalies d, e arba f punktą, kompetentingos institucijos nurodo prašymo tikslą ir patikslina prašomą informaciją.	**KSĮ projektas** **27 straipsnis. Bendrieji kibernetinio saugumo subjektų patikrinimų atlikimo pagrindai** <...>	Visiškas

	3. Atlikdamas šio įstatymo 26 straipsnio 1 dalyje nurodytus patikrinimus, Nacionalinis kibernetinio saugumo centras turi teisę: **<...>** **3) duoti nurodymus pateikti visą reikalingą informaciją, dokumentų kopijas ir išrašus, duomenų kopijas, taip pat susipažinti su visais duomenimis ir dokumentais, reikalingais kibernetinio saugumo subjektų tinklų ir informacinių sistemų atitikčiai šio įstatymo 14 straipsnio 1 dalyje nurodytiems reikalavimams įvertinti, įskaitant atliktų kibernetinio saugumo auditų rezultatus, įrodančius tinklų ir informacinių sistemų atitiktį nurodytiems reikalavimams;** **<...>** **5. Taikant šio straipsnio 3 dalies 3 punktą, Nacionalinis kibernetinio saugumo centras privalo nurodyti konkretų prašymo tikslą, pagrindą ir tiksliai apibrėžti prašomą informaciją.**	
4. Valstybės narės užtikrina, kad kompetentingos institucijos, naudodamosi savo vykdymo užtikrinimo įgaliojimais svarbių subjektų atžvilgiu, turėtų bent šiuos įgaliojimus: a) teikti įspėjimus, kad atitinkami subjektai pažeidžia šią direktyvą; b) priimti privalomus nurodymus arba įsakymą, kuriuo reikalaujama, kad atitinkami subjektai pašalintų nustatytus trūkumus arba ištaisytų šios direktyvos pažeidimą; c) nurodyti atitinkamiems subjektams nutraukti veiksmus, kurie pažeidžia šią direktyvą, ir tokių veiksmų nebekartoti; d) nurodyti atitinkamiems subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų kibernetinio saugumo rizikos valdymo priemonės atitiktų 21 straipsnį arba kad jie įvykdytų 23 straipsnyje nustatytas pareigas pranešti; e) įpareigoti atitinkamus subjektus informuoti fizinius arba juridinius asmenis, kuriems jie teikia paslaugas arba vykdo veiklą ir kuriuos gali paveikti didelė kibernetinė grėsmė, apie grėsmės pobūdį, taip pat apie visas galimas apsaugos ar taisomąsias priemones, kurių gali imtis tie fiziniai ar juridiniai asmenys, reaguodami į tą grėsmę; f) įpareigoti atitinkamus subjektus per pagrįstą terminą įgyvendinti saugumo audito metu pateiktas rekomendacijas;	**KSĮ projektas** **28 straipsnis. Vykdymo užtikrinimo priemonės** **1. Nacionalinis kibernetinio saugumo centras, šio įstatymo 26 straipsnio 1 dalyje nurodyto patikrinimo metu nustatęs šio įstatymo pažeidimą, taiko vykdymo užtikrinimo priemonę ar jų grupę:** **1) teikia įspėjimus, kad kibernetinio saugumo subjektai pažeidžia šio įstatymo nustatytus reikalavimus;** **2) duoda nurodymus esminiams subjektams dėl priemonių, kurių reikia siekiant užkirsti kelią kibernetiniam incidentui arba jam suvaldyti, ir tokių priemonių įgyvendinimo bei jų įgyvendinimo ataskaitų pateikimo terminų, nurodymus kibernetinio saugumo subjektams, kad atitinkami subjektai pašalintų nustatytus trūkumus arba ištaisytų šio įstatymo reikalavimų pažeidimus;** **3) duoda nurodymus kibernetinio saugumo subjektams nutraukti veiksmus, kurie pažeidžia šio įstatymo nustatytus reikalavimus, ir tokių veiksmų nebekartoti;** **4) duoda nurodymus kibernetinio saugumo subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų naudojamos kibernetinio saugumo rizikos valdymo priemonės atitiktų šio įstatymo 14 straipsnio 1 dalyje nurodytus teisės aktus arba kad jie įvykdytų šio įstatymo 18 straipsnio 1 dalyje nustatytą pareigą pranešti apie kibernetinius incidentus;** **5) duoda nurodymus kibernetinio saugumo subjektams informuoti fizinius arba juridinius asmenis, kuriems jie teikia paslaugas arba vykdo jiems**	Visiškas

g) įpareigoti atitinkamus subjektus konkrečiu būdu viešai paskelbti šios direktyvos pažeidimo aspektus; h) skirti arba prašyti, kad atitinkamos įstaigos ar teismai pagal nacionalinę teisę skirtų administracinę baudą pagal 34 straipsnį, kartu su bet kuriomis šios dalies a–g punktuose nurodytomis priemonėmis.	**aktualią veiklą ir kuriuos didelė kibernetinė grėsmė gali paveikti, apie grėsmės pobūdį, taip pat apie visus galimus veiksmus, kurių gali imtis tie fiziniai ar juridiniai asmenys, reaguodami į tą grėsmę;** **6) duoda nurodymus kibernetinio saugumo subjektams per pagrįstą terminą įgyvendinti kibernetinio saugumo audito metu pateiktas rekomendacijas;** **7) paskiria stebėsenos pareigūną, kuriam per nustatytą laikotarpį pavestos aiškiai apibrėžtos užduotys, prižiūrėti, kaip esminiai subjektai laikosi šio įstatymo 14 ir 18 straipsnių reikalavimų;** **8) duoda nurodymus kibernetinio saugumo subjektams konkrečiu būdu viešai paskelbti šio įstatymo pažeidimo aspektus;** **9) skiria kibernetinio saugumo subjektams baudą šio įstatymo 30 ir 31 straipsniuose nustatyta tvarka, kartu su bet kuriomis šios dalies 1–8, 10 ir 11 punktuose nurodytomis priemonėmis;** **10) inicijuoja šio įstatymo 32 straipsnyje nustatytą laikiną teisės užsiimti dalimi ar visa esminio subjekto vykdoma veikla ar teikti paslaugas sustabdymą;** **11) inicijuoja šio įstatymo 33 straipsnyje nustatytą esminio subjekto vadovo, išskyrus Lietuvos Respublikos Seimo, Vyriausybės ir Prezidento sprendimu skiriamus viešojo administravimo subjektų vadovus, laikiną nušalinimą nuo pareigų.**	
5. 32 straipsnio 6, 7 ir 8 dalys mutatis mutandis taikomos šiame straipsnyje numatytoms priežiūros ir vykdymo užtikrinimo priemonėms, skirtoms svarbiems subjektams.	**KSĮ projektas** **14 straipsnis. Kibernetinio saugumo rizikos valdymo priemonės** **<...>** **6. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo privalo užtikrinti, kad kibernetinio saugumo subjektas laikytųsi šiame įstatyme jam nustatytų pareigų, ir prižiūrėti jų laikymąsi. Kibernetinio saugumo subjekto vadovas, įgaliodamas šioje dalyje nurodytą asmenį, užtikrina, kad jis turėtų būtinų priemonių, reikalingų nurodytam įgaliojimui vykdyti.** **15 straipsnis. Už kibernetinį saugumą atsakingi asmenys** **1. Kibernetinio saugumo subjekto vadovas ar jo įgaliotas asmuo privalo paskirti kibernetinio saugumo vadovą, tiesiogiai atskaitingą kibernetinio saugumo subjekto vadovui, atsakingą už atitikties šio įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantį kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas.**	Visiškas

	2. Kibernetinio saugumo subjekto vadovas ar jo įgaliotas asmuo privalo paskirti saugos įgaliotinį, atsakingą už konkrečios tinklų ir informacinės sistemos atitiktį šio įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams ir atliekantį kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas. **3. Kibernetinio saugumo vadovas gali vykdyti saugos įgaliotinio funkcijas. Kibernetinio saugumo vadovas gali būti paskirtas atsakingas už šio įstatymo 14 ir 18 straipsniuose nustatytų reikalavimų, taikomų keliems kibernetinio saugumo subjektams, gyvendinimą. Saugos įgaliotinis gali būti paskirtas atsakingas už kelių tinklų ir informacinių sistemų atitiktį šio įstatymo 14 straipsnyje nustatytiems reikalavimams. Sprendimą dėl šioje dalyje numatytų už kibernetinį saugumą atsakingų asmenų skyrimo priima kibernetinio saugumo subjekto vadovas, atsižvelgdamas į kibernetinio saugumo subjekto organizacinę struktūrą ir dydį.** **28 straipsnis. Vykdymo užtikrinimo priemonės** <...> **3. Taikydamas bet kurią iš šio straipsnio 1 dalyje nurodytų vykdymo užtikrinimo priemonių, Nacionalinis kibernetinio saugumo centras atsižvelgia į kiekvieno konkretaus atvejo aplinkybes, taip pat į:** **1) atsakomybę lengvinančias aplinkybes, nustatytas šio straipsnio 4 dalyje, atsakomybę sunkinančias aplinkybės, nustatytas šio straipsnio 5 dalyje, ir pažeistų nuostatų pavojingumą, nurodytą šio įstatymo 29 straipsnyje;2) pažeidimo trukmę;** **3) subjekto įvykdytus ankstesnius šio įstatymo pažeidimus per pastaruosius 2 metus;** **4) padarytą turtinę arba neturtinę žalą, kuri vertinama apskaičiuojant finansinius ar ekonominius nuostolius, poveikį kitoms paslaugoms ir paveiktų naudotojų skaičių, nuostolių atlyginimą ar padaryto neigiamo poveikio panaikinimo;** **5) priemones, kurių subjektas ėmėsi siekdamas užkirsti kelią turtinei ar neturtinei žalai arba ją sumažinti;** **6) patvirtintų elgesio kodeksų arba patvirtintų sertifikavimo mechanizmų laikymąsi;** **7) bendradarbiavimą su Nacionaliniu kibernetinio saugumo centru;** **8) pažeidimo mastą.**	

	4. Šio straipsnio 3 dalies 1 punkte nurodytomis atsakomybę lengvinančiomis aplinkybėmis laikoma: **1) subjektas savo noru užkirto kelią turtinei ar neturtinei žalai;** **2) subjektas atlygino padarytą žalą;** **3) subjektas pripažino pažeidimą ir padėjo Nacionaliniam kibernetinio saugumo centrui patikrinimo metu;** **4) subjektas savo valia nutraukė pažeidimą;** **5) pažeidimas padarytas dėl neatsargumo;** **6) subjekto, kuris yra ūkio subjektas, finansinė padėtis yra labai sunki.** **5. Šio straipsnio 3 dalies 1 punkte nurodytomis atsakomybę sunkinančiomis aplinkybėmis laikoma:** **1) pažeidimas padarytas pakartotinai.. Laikoma, kad pažeidimas padarytas pakartotinai, jeigu subjektas, įtariamas pažeidimo padarymu, per paskutinius 12 mėnesių nuo sprendimo, kuriuo buvo paskirta vykdymo užtikrinimo priemonė, įsigaliojimo dienos padarė tokį patį pažeidimą. Padarius pakartotinį pažeidimą, šioje dalyje nustatytas terminas skaičiuojamas iš naujo;** **2) padarytas pavojingas pažeidimas, kaip jis suprantamas pagal šio įstatymo 29 straipsnio 2 dalį;** **3) subjektas neištaisė trūkumų pagal Nacionalinio kibernetinio saugumo centro pateiktus nurodymus;** **4) subjektas trukdė vykdyti kibernetinio saugumo audito ar stebėsenos pareigūno veiklą, kurią įpareigojo atlikti Nacionalinis kibernetinio saugumo centras, nustatęs pažeidimą;** **5) subjektas pateikė neteisingą informaciją, susijusios su šio įstatymo reikalavimais;** **6) subjektas slėpė padarytą pažeidimą ar pažeidimą tęsė nepaisant to, kad Nacionalinis kibernetinio saugumo centras buvo atkreipęs dėmesį į pažeidimus ar veiklos trūkumus.** **27 straipsnis. Bendrieji kibernetinio saugumo subjektų patikrinimų atlikimo pagrindai** <...> **8. Prieš priimdamas sprendimą taikyti šio įstatymo 28 straipsnio 1 dalyje nurodytą vykdymo užtikrinimo priemonę (priemones), Nacionalinis kibernetinio saugumo centras privalo apie tai informuoti kibernetinio saugumo subjektą, kuriam ketinama taikyti vykdymo užtikrinimo priemonę (priemones),**	

	pateikdamas esminę informaciją apie teisės aktų nuostatas ir nustatytus faktinius duomenis, kurie sudaro vykdymo užtikrinimo priemonės (priemonių) taikymo pagrindus, ir nustatyti ne trumpesnį kaip 20 darbo dienų terminą nuo pranešimo įteikimo dienos paaiškinimams pateikti, išskyrus atvejus, kai tai trukdytų imtis neatidėliotinų kibernetinių incidentų prevencijos arba reagavimo į juos veiksmų. Skiriant šio įstatymo 28 straipsnio 1 dalies 9-11 punktuose numatytas poveikio priemones šioje dalyje nurodytas 20 darbo dienų terminas paaiškinimams teikti privalo būti nustatomas. **ANK projektas** **„480 straipsnis. Lietuvos Respublikos kibernetinio saugumo įstatyme nustatytų kibernetinio saugumo užtikrinimo pareigų atlikimo pažeidimai** **<...>** **3. Lietuvos Respublikos kibernetinio saugumo įstatyme nustatytų reikalavimų kibernetinio saugumo subjektų vadovams ar jų įgaliotiems asmenims pažeidimas** **užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar jų įgaliotiems asmenims nuo dviejų šimtų penkiasdešimt iki trijų tūkstančių eurų.** **4. Šio straipsnio 3 dalyje numatytas administracinis nusižengimas, padarytas pakartotinai,** **užtraukia baudą nuo dviejų tūkstančių iki šešių tūkstančių eurų.“**	
6. Valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą bendradarbiautų su atitinkamomis atitinkamos valstybės narės kompetentingomis institucijomis pagal Reglamentą (ES) 2022/2554. Visų pirma valstybės narės užtikrina, kad jų kompetentingos institucijos pagal šią direktyvą informuotų Priežiūros forumą, įsteigtą pagal Reglamento (ES) 2022/2554 32 straipsnio 1 dalį, kai jos naudojasi priežiūros ir vykdymo užtikrinimo įgaliojimais, kuriais siekiama užtikrinti, kad svarbus subjektas, paskirtas ypatingai svarbiu trečiųjų šalių IRT paslaugų teikėju pagal Reglamento (ES) 2022/2554 31 straipsnį, laikytųsi šios direktyvos.	**KSĮ projektas** **20 straipsnis. Tarpinstitucinis bendradarbiavimas** **<...>** **2. Nacionalinis kibernetinio saugumo centras:** **<...>** **2) ne vėliau kaip per 20 darbo dienų nuo sprendimo taikyti šio įstatymo 28 straipsnio 1 dalyje vykdymo užtikrinimo priemonę priėmimo apie tai informuoja kompetentingą instituciją pagal Reglamentą (ES) 2022/2554, jeigu vykdymo užtikrinimo priemonė taikoma siekiant užtikrinti, kad esminis subjektas, kuris paskirtas ypatingai svarbiu trečiųjų šalių informacinių ir ryšių technologijų paslaugų teikėju pagal Reglamento (ES) 2022/2554 31 straipsnį, laikytųsi šio įstatymo reikalavimų.**	Visiškas
34 straipsnis. Bendrosios administracinių baudų skyrimo esminiams ir svarbiems subjektams sąlygos		

1. Valstybės narės užtikrina, kad už šios direktyvos pažeidimus esminiams ir svarbiems subjektams skiriamos administracinės baudos pagal šį straipsnį kiekvienu atskiru atveju būtų veiksmingos, proporcingos ir atgrasomos, atsižvelgiant į kiekvieno konkretaus atvejo aplinkybes.	**KSĮ projektas** **29 straipsnis. Pažeidimai, dėl kurių taikomos vykdymo užtikrinimo priemonės** **1. Pažeidimais yra laikomi šiame įstatyme ir jį įgyvendinančiuose teisės aktuose nustatytų reikalavimų nesilaikymas ar trukdymas šio įstatymo 4 straipsnio 2 ir 3 dalyse nurodytoms institucijoms, įskaitant jų pasitelktus subjektus, atlikti joms priskirtas funkcijas. Pažeidimai skirstomi į: pavojingus, vidutinio pavojingumo, nedidelio pavojingumo.** **2. Pažeidimais, priskiriamais pavojingiems pažeidimams, yra laikomi šio įstatymo 14 straipsnio 1 dalyje, 18 straipsnio 1 dalies 1 punkte nustatytų reikalavimų pažeidimai.** **3. Pažeidimais, priskiriamais vidutinio pavojingumo pažeidimams, yra laikomi šio įstatymo 7 straipsnio 2 dalies 6 ir 7 dalyse, 14 straipsnio 6 ir 8 dalyse, 15 straipsnio 1, 2 ir 3 dalyse, nustatytų reikalavimų pažeidimai ar trukdymas institucijoms atlikti šio įstatymo 27 straipsnio 3 dalyje joms priskirtas funkcijas, taip pat šio įstatymo 17 straipsnyje nustatytų reikalavimų pažeidimai, jeigu juos atliko aukščiausio lygio domenų vardų registro paslaugas teikiantis subjektai.** **4. Pažeidimais, priskiriamais nedidelio pavojingumo pažeidimams, yra laikomi šio įstatymo 14 straipsnio 3 ir 7 dalyse, 18 straipsnio 1 dalies 2 punkte, 19 straipsnio 4 dalyje nustatytų reikalavimų pažeidimai, taip pat šio įstatymo 17 straipsnyje nustatytų reikalavimų pažeidimai, jeigu juos atliko domenų vardų registro paslaugas teikiantis subjektai.** **30 straipsnis. Baudos** **1. Baudas skiria Nacionalinio kibernetinio saugumo centro vadovas ar jo įgaliotas asmuo pagal vykdymo užtikrinimo priemonių taikymo esminiams ir svarbiems subjektams tvarką, tvirtinamą Vyriausybės.** **2. Už 29 straipsnyje nurodytus pažeidimus skiriamų baudų dydžiai:** **1) esminiam subjektui – iki 10 000 000 Eur arba iki 2 proc. juridinio asmens bendros pasaulinės metinės apyvartos per praėjusį finansinį laikotarpį, atsižvelgiant į tai, kuri suma didesnė;** **2) svarbiam subjektui – iki 7 000 000 Eur arba iki 1,4 proc. juridinio asmens bendros pasaulinės metinės apyvartos per praėjusį finansinį laikotarpį, atsižvelgiant į tai, kuri suma didesnė;** **3) biudžetinei įstaigai, kuri yra esminis subjektas – iki 1 procento biudžetinės įstaigos einamųjų metų biudžeto ir kitų praėjusiais metais gautų bendrųjų metinių pajamų dydžio, bet ne didesnė negu 60 000 Eur;**	Visiškas

	4) biudžetinei įstaigai, kuri yra svarbus subjektas – iki 0,5 procento biudžetinės įstaigos einamųjų metų biudžeto ir kitų praėjusiais metais gautų bendrųjų metinių pajamų dydžio, bet ne didesnė negu 30 000 Eur. **3. Nustatomos šios baudos:** **1) iki 100 proc. šio straipsnio 2 dalyje nustatytos maksimalios baudos, jei pažeidimas yra laikomas pavojingu pažeidimu pagal šio įstatymo 29 straipsnio 2 dalį;** **2) iki 50 proc. šio straipsnio 2 dalyje nustatytos maksimalios baudos, jei pažeidimas yra laikomas vidutinio pavojingumo pažeidimu pagal šio įstatymo 29 straipsnio 3 dalį;** **3) iki 10 proc. šio straipsnio 2 dalyje nustatytos maksimalios baudos, jei pažeidimas yra laikomas nedidelio pavojingumo pažeidimu pagal šio įstatymo 29 straipsnio 4 dalį.** **4. Nustatomas konkretus baudos dydis turi būti veiksmingas, proporcingas padarytam pažeidimui ir atgrasantis nuo pažeidimų darymo ateityje. Nustatant konkretų baudos dydį atsižvelgiama į 28 straipsnio 3 dalyje nurodytas aplinkybes, išskyrus 28 straipsnio 4 dalies 2 punkte nurodytą aplinkybę.**	
2. Administracinės baudos skiriamos kartu su 32 straipsnio 4 dalies a–h punktuose, 32 straipsnio 5 dalyje ir 33 straipsnio 4 dalies a–g punktuose nurodytomis priemonėmis.	**KSĮ projektas** **28 straipsnis. Vykdymo užtikrinimo priemonės** **1. Nacionalinis kibernetinio saugumo centras, šio įstatymo 26 straipsnio 1 dalyje nurodyto patikrinimo metu nustatęs šio įstatymo pažeidimą, taiko vykdymo užtikrinimo priemonę ar jų grupę:** <...> **9) skiria kibernetinio saugumo subjektams baudą šio įstatymo 30 ir 31 straipsniuose nustatyta tvarka, kartu su bet kuriomis šios dalies 1–8, 10 ir 11 punktuose nurodytomis priemonėmis.**	Visiškas
3. Sprendžiant, ar skirti administracinę baudą, ir kiekvienu konkrečiu atveju priimant sprendimą dėl jos dydžio, deramai atsižvelgiama bent į 32 straipsnio 7 dalyje nurodytus aspektus.	**KSĮ projektas** **28 straipsnis. Vykdymo užtikrinimo priemonės** <...> **3. Taikydamas bet kurią iš šio straipsnio 1 dalyje nurodytų vykdymo užtikrinimo priemonių, Nacionalinis kibernetinio saugumo centras atsižvelgia į kiekvieno konkretaus atvejo aplinkybes, taip pat į:** **1) atsakomybę sunkinančias aplinkybes, nustatytas šio straipsnio 4 dalyje, ir pažeistų nuostatų pavojingumą, nurodytą šio įstatymo 29 straipsnyje;** **2) pažeidimo trukmę;**	Visiškas

	3) subjekto įvykdytus ankstesnius šio įstatymo pažeidimus per pastaruosius 2 metus; **4) padarytą turtinę arba neturtinę žalą, kuri vertinama apskaičiuojant finansinius ar ekonominius nuostolius, poveikį kitoms paslaugoms ir paveiktų naudotojų skaičių, nuostolių atlyginimą ar padaryto neigiamo poveikio panaikinimo;** **5) tai, ar pažeidimą įvykdęs subjektas veikė tyčia ar pažeidimas padarytas dėl neatsargumo;** **6) priemones, kurių subjektas ėmėsi siekdamas užkirsti kelią turtinei ar neturtinei žalai arba ją sumažinti;** **7) patvirtintų elgesio kodeksų arba patvirtintų sertifikavimo mechanizmų laikymąsi;** **8) bendradarbiavimą su Nacionaliniu kibernetinio saugumo centru;** **9) pažeidimo mastą.** **4. Šio straipsnio 3 dalies 1 punkte nurodytomis atsakomybę sunkinančiomis aplinkybėmis laikoma:** **1) pakartotiniai pažeidimai. Laikoma, kad pažeidimas padarytas pakartotinai, jeigu subjektas, įtariamas pažeidimo padarymu, per paskutinius 12 mėnesių nuo sprendimo, kuriuo buvo paskirta vykdymo užtikrinimo priemonė, įsigaliojimo dienos padarė tokį patį pažeidimą. Padarius pakartotinį pažeidimą, šioje dalyje nustatytas terminas skaičiuojamas iš naujo;** **2) pavojingi pažeidimai, kaip jie suprantami pagal šio įstatymo 29 straipsnio 2 dalį;** **3) trūkumų pagal Nacionalinio kibernetinio saugumo centro pateiktus nurodymus neištaisymas;** **4) trukdymas vykdyti kibernetinio saugumo audito ar stebėsenos pareigūno veiklą, kurią įpareigojo atlikti Nacionalinis kibernetinio saugumo centras, nustatęs pažeidimą;** **5) neteisingos informacijos, susijusios su šio įstatymo reikalavimais, pateikimas;** **6) padaryto pažeidimo slėpimas, pažeidimo tęsimas nepaisant to, kad Nacionalinis kibernetinio saugumo centras buvo atkreipęs dėmesį į pažeidimus ar veiklos trūkumus.**	
4. Valstybės narės užtikrina, kad už 21 arba 23 straipsnio pažeidimus pagal šio straipsnio 2 ir 3 dalis esminiams subjektams būtų skiriamos administracinės baudos, kurių didžiausia būtų	**KSĮ projektas** **30 straipsnis. Baudos** <...>	Visiškas

bent 10 000 000 EUR arba kurių didžiausia būtų bent 2 proc. įmonės, kuriai tas esminis subjektas priklauso, bendros pasaulinės metinės apyvartos praėjusiais finansiniais metais, atsižvelgiant į tai, kuri suma yra didesnė.	**2. Už 29 straipsnyje nurodytus pažeidimus skiriamų baudų dydžiai:** **1) esminiam subjektui – iki 10 000 000 Eur arba iki 2 proc. juridinio asmens bendros pasaulinės metinės apyvartos per praėjusį finansinį laikotarpį, atsižvelgiant į tai, kuri suma didesnė;** **2) svarbiam subjektui – iki 7 000 000 Eur arba iki 1,4 proc. juridinio asmens bendros pasaulinės metinės apyvartos per praėjusį finansinį laikotarpį, atsižvelgiant į tai, kuri suma didesnė;** **3) biudžetinei įstaigai, kuri yra esminis subjektas – iki 1 procento biudžetinės įstaigos einamųjų metų biudžeto ir kitų praėjusiais metais gautų bendrųjų metinių pajamų dydžio, bet ne didesnė negu 60 000 Eur;** **4) biudžetinei įstaigai, kuri yra svarbus subjektas – iki 0,5 procento biudžetinės įstaigos einamųjų metų biudžeto ir kitų praėjusiais metais gautų bendrųjų metinių pajamų dydžio, bet ne didesnė negu 30 000 Eur.** **3. Nustatomos šios baudos:** **1) iki 100 proc. šio straipsnio 2 dalyje nustatytos maksimalios baudos, jei pažeidimas yra laikomas pavojingu pažeidimu pagal šio įstatymo 29 straipsnio 2 dalį;** **2) iki 50 proc. šio straipsnio 2 dalyje nustatytos maksimalios baudos, jei pažeidimas yra laikomas vidutinio pavojingumo pažeidimu pagal šio įstatymo 29 straipsnio 3 dalį;** **3) iki 10 proc. šio straipsnio 2 dalyje nustatytos maksimalios baudos, jei pažeidimas yra laikomas nedidelio pavojingumo pažeidimu pagal šio įstatymo 29 straipsnio 4 dalį.**	
5. Valstybės narės užtikrina, kad už 21 arba 23 straipsnio pažeidimus pagal šio straipsnio 2 ir 3 dalis svarbiems subjektams būtų skiriamos administracinės baudos, kurių didžiausia būtų bent 7 000 000 EUR arba kurių didžiausia būtų bent 1,4 proc. įmonės, kuriai tas svarbus subjektas priklauso, bendros pasaulinės metinės apyvartos praėjusiais finansiniais metais, atsižvelgiant į tai, kuri suma yra didesnė.		
6. Valstybės narės gali numatyti įgaliojimą skirti periodines baudas, siekiant priversti esminį arba svarbų subjektą nutraukti šios direktyvos pažeidimą, remiantis išankstiniu kompetentingos institucijos sprendimu.	*Lietuva nėra pasirinkusi įgyvendinti šios direktyvos nuostatos*	
7. Nedarant poveikio kompetentingų institucijų įgaliojimams pagal 32 ir 33 straipsnius, kiekviena valstybė narė gali nustatyti taisykles dėl to, ar ir kokiu mastu administracinės baudos gali būti skiriamos viešojo administravimo subjektams, kuriems taikomos šioje direktyvoje nustatytos pareigos.	**KSĮ projektas** **30 straipsnis. Baudos** **<...>** **2. Už 29 straipsnyje nurodytus pažeidimus skiriamų baudų dydžiai:** **<...>** **3) biudžetinei įstaigai, kuri yra esminis subjektas – iki 1 procento biudžetinės įstaigos einamųjų metų biudžeto ir kitų praėjusiais metais gautų bendrųjų metinių pajamų dydžio, bet ne didesnė negu 60 000 Eur;**	Visiškas

	4) biudžetinei įstaigai, kuri yra svarbus subjektas – iki 0,5 procento biudžetinės įstaigos einamųjų metų biudžeto ir kitų praėjusiais metais gautų bendrųjų metinių pajamų dydžio, bet ne didesnė negu 30 000 Eur. **<...>** **4. Nustatomas konkretus baudos dydis turi būti veiksmingas, proporcingas padarytam pažeidimui ir atgrasantis nuo pažeidimų darymo ateityje. Nustatant konkretų baudos dydį atsižvelgiama į 28 straipsnio 3 dalyje nurodytas aplinkybes, išskyrus 28 straipsnio 4 dalies 2 punkte nurodytą aplinkybę.** **ANK projektas** **„480 straipsnis. Lietuvos Respublikos kibernetinio saugumo įstatyme nustatytų kibernetinio saugumo užtikrinimo pareigų atlikimo pažeidimai** **<...>** **3. Lietuvos Respublikos kibernetinio saugumo įstatyme nustatytų reikalavimų kibernetinio saugumo subjektų vadovams ar jų įgaliotiems asmenims pažeidimas** **užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar jų įgaliotiems asmenims nuo dviejų šimtų penkiasdešimt iki trijų tūkstančių eurų.** **4. Šio straipsnio 3 dalyje numatytas administracinis nusižengimas, padarytas pakartotinai,** **užtraukia baudą nuo dviejų tūkstančių iki šešių tūkstančių eurų.“**	
8. Jei valstybės narės teisės sistemoje nenumatoma administracinių baudų, ta valstybė narė užtikrina, kad šis straipsnis galėtų būti taikomas taip, kad baudą inicijuotų kompetentinga institucija, o ją skirtų kompetentingi nacionaliniai teismai arba specialios jurisdikcijos teismai, sykiu užtikrinant, kad tos teisių gynimo priemonės būtų veiksmingos ir turėtų kompetentingų institucijų skiriamoms administracinėms baudoms lygiavertį poveikį. Bet kuriuo atveju skiriamos baudos turi būti veiksmingos, proporcingos ir atgrasomosios. Valstybė narė ne vėliau kaip 2024 m. spalio 17 d. praneša Komisijai apie įstatymų, kuriuos ji priima pagal šią dalį, nuostatas ir nedelsdama praneša apie visus vėlesnius tas nuostatas keičiančius teisės aktus arba joms įtakos turinčius pakeitimus.	*Lietuva nėra pasirinkusi įgyvendinti šios direktyvos nuostatos*	

35 straipsnis. Pažeidimai, susiję su asmens duomenų saugumo pažeidimu		
1. Jeigu, vykdydamos priežiūrą ar vykdymo užtikrinimą, kompetentingos institucijos išsiaiškina, kad dėl esminio arba svarbaus subjekto padaryto šios direktyvos 21 ir 23 straipsniuose nustatytų pareigų pažeidimo gali būti padarytas asmens duomenų saugumo pažeidimas, kaip apibrėžta Reglamento (ES) 2016/679 4 straipsnio 12 punkte, apie kurį turi būti pranešta pagal to reglamento 33 straipsnį, jos, nepagrįstai nedelsdamos, informuoja priežiūros institucijas, kaip nurodyta to reglamento 55 arba 56 straipsnyje.	**KSĮ projektas** **20 straipsnis. Tarpinstitucinis bendradarbiavimas** **<...>** **2. Nacionalinis kibernetinio saugumo centras:** **<...>** **4) nustatęs, kad esminis ar svarbus subjektas gali būti padaręs asmens duomenų saugumo pažeidimą, apie tai nepagrįstai nedelsiant, bet ne vėliau kaip per 72 valandas nuo šios aplinkybės nustatymo, informuoja Valstybinę duomenų apsaugos inspekciją nurodydamas turimą informaciją apie Reglamento (ES) 2016/679 33 straipsnio 3 dalyje nurodytas aplinkybes.**	Visiškas
2. Jeigu priežiūros institucijos, kaip nurodyta Reglamento (ES) 2016/679 55 arba 56 straipsnyje, skiria administracinę baudą pagal to reglamento 58 straipsnio 2 dalies i punktą, kompetentingos institucijos negali skirti administracinės baudos pagal šios direktyvos 34 straipsnį už šio straipsnio 1 dalyje nurodytą pažeidimą, įvykdytą tuo pačiu elgesiu, už kurį buvo skirta administracinė bauda pagal Reglamento (ES) 2016/679 58 straipsnio 2 dalies i punktą. Tačiau kompetentingos institucijos gali taikyti šios direktyvos 32 straipsnio 4 dalies a–h punktuose, 32 straipsnio 5 dalyje ir 33 straipsnio 4 dalies a–g punktuose numatytas vykdymo užtikrinimo priemones.	**KSĮ projektas** **31 straipsnis. Baudų skyrimo tvarka** **<...>** **13. Bauda neskiriama, jeigu kibernetinio saugumo subjektui už tą patį pažeidimą jau buvo skirta bauda vadovaujantis Reglamento (ES) 2016/679 58 straipsnio 2 dalies i punktu.**	Visiškas
3. Jeigu priežiūros institucija, kompetentinga pagal Reglamentą (ES) 2016/679, yra įsteigta kitoje valstybėje narėje nei kompetentinga institucija, kompetentinga institucija apie 1 dalyje nurodytą galimą duomenų pažeidimą informuoja jos pačios valstybėje narėje įsteigtą priežiūros instituciją.	**KSĮ projektas** **20 straipsnis. Tarpinstitucinis bendradarbiavimas** **<...>** **2. Nacionalinis kibernetinio saugumo centras:** **<...>** **4) nustatęs, kad esminis ar svarbus subjektas gali būti padaręs asmens duomenų saugumo pažeidimą, apie tai nepagrįstai nedelsiant, bet ne vėliau kaip per 72 valandas nuo šios aplinkybės nustatymo, informuoja Valstybinę duomenų apsaugos inspekciją nurodydamas turimą informaciją apie Reglamento (ES) 2016/679 33 straipsnio 3 dalyje nurodytas aplinkybes.**	Visiškas
36 straipsnis. Sankcijos		

Valstybės narės nustato sankcijų, taikomų pažeidus pagal šią direktyvą priimtas nacionalines nuostatas, taisykles ir imasi visų būtinų priemonių užtikrinti, kad šios sankcijos būtų įgyvendinamos. Numatytos sankcijos turi būti veiksmingos, proporcingos ir atgrasomos. Valstybės narės ne vėliau kaip 2025 m. sausio 17 d. praneša Komisijai apie tas taisykles ir priemones ir nepagrįstai nedelsdamos informuoja ją apie visus vėlesnius joms įtakos turinčius pakeitimus.	**KSĮ projektas** **27 straipsnis. Bendrieji kibernetinio saugumo subjektų patikrinimų atlikimo pagrindai** **<...>** **6. Nacionalinis kibernetinio saugumo centras, baigęs patikrinimą, priima bent vieną iš šių sprendimų:** **1) konstatuoti, kad pažeidimų nenustatyta;** **2) nustatęs šio įstatymo pažeidimą, taikyti šio įstatymo 28 straipsnyje nurodytas vykdymo užtikrinimo priemones.** **7. Nustačius šio įstatymo pažeidimą, šio įstatymo 28 straipsnyje numatytos vykdymo užtikrinimo priemonės, išskyrus nurodytas 28 straipsnio 1 dalies 9-11 punktuose, atsižvelgiant į patikrinimo sudėtingumą, mastą, kibernetinio saugumo subjektų veiklos pobūdį bei vengimą vykdyti Nacionalinio kibernetinio saugumo centro reikalavimus, patikrinimo metu paaiškėjusias naujas aplinkybes arba kitas objektyvias priežastis, gali būti taikomos ir nebaigus patikrinimo.** **28 straipsnis. Vykdymo užtikrinimo priemonės** **1. Nacionalinis kibernetinio saugumo centras, šio įstatymo 26 straipsnio 1 dalyje nurodyto patikrinimo metu nustatęs šio įstatymo pažeidimą, taiko vykdymo užtikrinimo priemonę ar jų grupę:** **1) teikia įspėjimus, kad kibernetinio saugumo subjektai pažeidžia šio įstatymo nustatytus reikalavimus;** **2) duoda nurodymus esminiams subjektams dėl priemonių, kurių reikia siekiant užkirsti kelią kibernetiniam incidentui arba jam suvaldyti, ir tokių priemonių įgyvendinimo bei jų įgyvendinimo ataskaitų pateikimo terminų, nurodymus kibernetinio saugumo subjektams, kad atitinkami subjektai pašalintų nustatytus trūkumus arba ištaisytų šio įstatymo reikalavimų pažeidimus;** **3) duoda nurodymus kibernetinio saugumo subjektams nutraukti veiksmus, kurie pažeidžia šio įstatymo nustatytus reikalavimus, ir tokių veiksmų nebekartoti;** **4) duoda nurodymus kibernetinio saugumo subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų naudojamos kibernetinio saugumo rizikos valdymo priemonės atitiktų šio įstatymo 14 straipsnio 1 dalyje nurodytus**	Visiškas

	teisės aktus arba kad jie įvykdytų šio įstatymo 18 straipsnio 1 dalyje nustatytą pareigą pranešti apie kibernetinius incidentus; **5) duoda nurodymus kibernetinio saugumo subjektams informuoti fizinius arba juridinius asmenis, kuriems jie teikia paslaugas arba vykdo jiems aktualią veiklą ir kuriuos didelė kibernetinė grėsmė gali paveikti, apie grėsmės pobūdį, taip pat apie visus galimus veiksmus, kurių gali imtis tie fiziniai ar juridiniai asmenys, reaguodami į tą grėsmę;** **6) duoda nurodymus kibernetinio saugumo subjektams per pagrįstą terminą įgyvendinti kibernetinio saugumo audito metu pateiktas rekomendacijas;** **7) paskiria stebėsenos pareigūną, kuriam per nustatytą laikotarpį pavestos aiškiai apibrėžtos užduotys, prižiūrėti, kaip esminiai subjektai laikosi šio įstatymo 14 ir 18 straipsnių reikalavimų;** **8) duoda nurodymus kibernetinio saugumo subjektams konkrečiu būdu viešai paskelbti šio įstatymo pažeidimo aspektus;** **9) skiria kibernetinio saugumo subjektams baudą šio įstatymo 30 ir 31 straipsniuose nustatyta tvarka, kartu su bet kuriomis šios dalies 1–8, 10 ir 11 punktuose nurodytomis priemonėmis;** **10) inicijuoja šio įstatymo 32 straipsnyje nustatytą laikiną teisės užsiimti dalimi ar visa esminio subjekto vykdoma veikla ar teikti paslaugas sustabdymą;** **11) inicijuoja šio įstatymo 33 straipsnyje nustatytą esminio subjekto vadovo, išskyrus Lietuvos Respublikos Seimo, Vyriausybės ir Prezidento sprendimu skiriamus viešojo administravimo subjektų vadovus, laikiną nušalinimą nuo pareigų.** **29 straipsnis. Pažeidimai, dėl kurių taikomos vykdymo užtikrinimo priemonės** **1. Pažeidimais yra laikomi šiame įstatyme ir jį įgyvendinančiuose teisės aktuose nustatytų reikalavimų nesilaikymas bei trukdymas šio įstatymo 4 straipsnio 2 ir 3 dalyse nurodytoms institucijoms, įskaitant jų pasitelktus asmenis, atlikti joms priskirtas funkcijas. Pažeidimai skirstomi į: pavojingus, vidutinio pavojingumo, nedidelio pavojingumo.** **2. Pažeidimais, priskiriamais pavojingiems pažeidimams, yra laikomi 14 straipsnio 1 dalyje, 18 straipsnio 1 dalies 1 punkte nustatytų reikalavimų pažeidimai.** **3. Pažeidimais, priskiriamais vidutinio pavojingumo pažeidimams, yra laikomi 7 straipsnio 2 dalies 6 ir 7 dalyse,14 straipsnio 6 ir 8 dalyse, 15 straipsnio**	

	1, 2 ir 3 dalyse, nustatytų reikalavimų pažeidimai ar trukdymas institucijoms atlikti šio įstatymo 27 straipsnio 3 dalyje joms priskirtas funkcijas, taip pat šio įstatymo 17 straipsnyje nustatytų reikalavimų pažeidimai, jeigu juos atliko aukščiausio lygio domenų vardų registro paslaugas teikiantis subjektai. **4. Pažeidimais, priskiriamais nedidelio pavojingumo pažeidimams, yra laikomi 14 straipsnio 3 ir 7 dalyse, 18 straipsnio 1 dalies 2 punkte, 19 straipsnio 4 dalyje nustatytų reikalavimų pažeidimai, taip pat šio įstatymo 17 straipsnyje nustatytų reikalavimų pažeidimai, jeigu juos atliko domenų vardų registro paslaugas teikiantis subjektai.** **30 straipsnis. Baudos** **1. Baudas skiria Nacionalinio kibernetinio saugumo centro vadovas ar jo įgaliotas asmuo pagal vykdymo užtikrinimo priemonių taikymo esminiams ir svarbiems subjektams tvarką, tvirtinamą Vyriausybės.** **2. Už 29 straipsnyje nurodytus pažeidimus skiriamų baudų dydžiai:** **1) esminiam subjektui – iki 10 000 000 Eur arba iki 2 proc. juridinio asmens bendros pasaulinės metinės apyvartos per praėjusį finansinį laikotarpį, atsižvelgiant į tai, kuri suma didesnė;** **2) svarbiam subjektui – iki 7 000 000 Eur arba iki 1,4 proc. juridinio asmens bendros pasaulinės metinės apyvartos per praėjusį finansinį laikotarpį, atsižvelgiant į tai, kuri suma didesnė;** **3) biudžetinei įstaigai, kuri yra esminis subjektas – iki 1 procento biudžetinės įstaigos einamųjų metų biudžeto ir kitų praėjusiais metais gautų bendrųjų metinių pajamų dydžio, bet ne didesnė negu 60 000 Eur;** **4) biudžetinei įstaigai, kuri yra svarbus subjektas – iki 0,5 procento biudžetinės įstaigos einamųjų metų biudžeto ir kitų praėjusiais metais gautų bendrųjų metinių pajamų dydžio, bet ne didesnė negu 30 000 Eur.** **3. Nustatomos šios baudos:** **1) iki 100 proc. šio straipsnio 2 dalyje nustatytos maksimalios baudos, jei pažeidimas yra laikomas pavojingu pažeidimu pagal šio įstatymo 29 straipsnio 2 dalį;** **2) iki 50 proc. šio straipsnio 2 dalyje nustatytos maksimalios baudos, jei pažeidimas yra laikomas vidutinio pavojingumo pažeidimu pagal šio įstatymo 29 straipsnio 3 dalį;**	

	3) iki 10 proc. šio straipsnio 2 dalyje nustatytos maksimalios baudos, jei pažeidimas yra laikomas nedidelio pavojingumo pažeidimu pagal šio įstatymo 29 straipsnio 4 dalį. **4. Nustatomas konkretus baudos dydis turi būti veiksmingas, proporcingas padarytam pažeidimui ir atgrasantis nuo pažeidimų darymo ateityje. Nustatant konkretų baudos dydį atsižvelgiama į 28 straipsnio 3 dalyje nurodytas aplinkybes, išskyrus 28 straipsnio 4 dalies 2 punkte nurodytą aplinkybę.**	
37 straipsnis. Savitarpio pagalba		
1. Kai subjektas teikia paslaugas daugiau nei vienoje valstybėje narėje arba teikia paslaugas vienoje ar daugiau valstybių narių, o jo tinklų ir informacinės sistemos yra vienoje ar daugiau kitų valstybių narių, atitinkamų valstybių narių kompetentingos institucijos viena su kita bendradarbiauja ir padeda viena kitai. Tas bendradarbiavimas apima bent tai, kad: a) valstybės narės kompetentingos institucijos, taikančios priežiūros arba vykdymo užtikrinimo priemones, per bendrąjį kontaktinį punktą informuoja kitų atitinkamų valstybių narių kompetentingas institucijas ir su jomis konsultuojasi dėl priežiūros ir vykdymo užtikrinimo priemonių, kurių imtasi; b) kompetentinga institucija gali prašyti kitos kompetentingos institucijos imtis priežiūros arba vykdymo užtikrinimo priemonių; c) kompetentinga institucija, gavusi kitos kompetentingos institucijos pagrįstą prašymą, teikia kitai kompetentingai institucijai savitarpio pagalbą, proporcingą jos pačios turimiems ištekliams, kad priežiūros ar vykdymo užtikrinimo priemonės galėtų būti įgyvendinamos veiksmingai, efektyviai ir nuosekliai. Pirmos pastraipos c punkte nurodyta savitarpio pagalba gali apimti prašymus pateikti informaciją ir priežiūros priemones, įskaitant prašymus atlikti patikrinimus vietoje arba priežiūrą ne vietoje, arba tikslinius saugumo auditus. Kompetentinga institucija, kuriai pateiktas pagalbos prašymas, negali atmesti to prašymo, išskyrus atvejus, kai nustatoma, kad ji neturi kompetencijos teikti prašomą pagalbą, prašoma pagalba nėra proporcinga kompetentingos institucijos priežiūros atliekamų	**KSĮ projektas** **20 straipsnis. Tarpinstitucinis bendradarbiavimas** **<...>** **2. Nacionalinis kibernetinio saugumo centras:** **<...>** **7) bendradarbiauja su kitų valstybių narių kompetentingomis institucijos, atsakingomis už kibernetinio saugumo reikalavimų vykdymo užtikrinimą, kai kibernetinio saugumo subjektas teikia paslaugas daugiau nei vienoje valstybėje narėje arba teikia paslaugas vienoje ar daugiau valstybių narių, o jo tinklų ir informacinės sistemos yra vienoje ar daugiau kitų valstybių narių, vykdydamos savitarpio pagalbos prašymus šios įstatymo 21 straipsnio nustatyta tvarka.** **21 straipsnis. Savitarpio pagalba** **1. Nacionalinis kibernetinio saugumo centras, gavęs kitos valstybės narės kompetentingos institucijos pagrįstą savitarpio prašymą, vykdo šio įstatymo 26 ir 28 straipsniuose numatytus kibernetinio saugumo subjektų patikrinimo ir (ar) vykdymo užtikrinimo priemonių veiksmus, taip pat kitus prašomus veiksmus, kuriuos vykdyti suteikia teisę šis įstatymas. Teikdamas savitarpio pagalbą dėl šio įstatymo 12 straipsnio 1 dalies 3 punkte nurodyto subjekto, kurio pagrindinė buveinė yra ne Lietuvos Respublikoje, Nacionalinis kibernetinio saugumo centras negali imtis daugiau veiksmų, nei nurodyta savitarpio pagalbos prašyme.** **2. Nacionalinis kibernetinio saugumo centras kitos valstybės narės kompetentingos institucijos savitarpio pagalbos prašymą gali atmesti tik tais atvejais kai:** **1) Nacionalinis kibernetinio saugumo centras neturi kompetencijos teikti prašomą pagalbą;**	Visiškas

užduočių atžvilgiu arba prašymas yra susijęs su informacija arba apima veiklą, kuri, ją atskleidus arba atlikus, prieštarautų tos valstybės narės nacionaliniam saugumui, visuomenės saugumui ar gynybai. Prieš atsisakydama patenkinti tokį prašymą, kompetentinga institucija konsultuojasi su kitomis atitinkamomis kompetentingomis institucijomis, taip pat, vienos iš atitinkamų valstybių narių prašymu, su Komisija ir ENISA. 2. Kai tinkama ir bendru sutarimu, skirtingų valstybių narių kompetentingos institucijos gali vykdyti bendrus priežiūros veiksmus.	**2) prašoma pagalba nėra proporcinga Nacionalinio kibernetinio saugumo centro turimiems žmogiškiesiems ar finansiniams ištekliams;** **3) prašymas yra susijęs su informacija arba apima veiklą, kurios atskleidimas arba atlikimas prieštarautų Lietuvos Respublikos nacionaliniam saugumui, visuomenės saugumui ar gynybai.** **3. Jeigu Nacionalinis kibernetinio saugumo centras pagal kompetenciją negali įgyvendinti pateikto savitarpio pagalbos prašymo, tačiau nustatęs, kad prašymą turėtų vykdyti kita valstybės institucija, prašymo nenagrinėja, persiunčia jį kitai valstybės institucijai ir apie tai praneša prašymą pateikusiai kitos valstybės kompetentingai institucijai.** **4. Nacionalinis kibernetinio saugumo centras negalėdamas įvykdyti kitos valstybės narės kompetentingos institucijos savitarpio pagalbos prašymo apie tai privalo ją informuoti, nurodydamas negalėjimo įgyvendinti prašymo priežastis, ir, jeigu yra kitos valstybės narės prašymas, prieš atmesdamas tokį prašymą, konsultuojasi su Europos Komisija ir (ar) Europos Sąjungos kibernetinio saugumo agentūra.**	
38 straipsnis. Įgaliojimų delegavimas		
1. Įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami šiame straipsnyje nustatytomis sąlygomis.	*Direktyvos straipsnio į nacionalinę teisę perkelti nereikia*	
2. 24 straipsnio 2 dalyje nurodyti įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami penkerių metų laikotarpiui nuo 2023 m. sausio 16 d.	*Direktyvos straipsnio į nacionalinę teisę perkelti nereikia*	
3. Europos Parlamentas arba Taryba gali bet kada atšaukti 24 straipsnio 2 dalyje nurodytus deleguotuosius įgaliojimus. Sprendimu dėl įgaliojimų atšaukimo nutraukiami tame sprendime nurodyti įgaliojimai priimti deleguotuosius aktus. Sprendimas įsigalioja kitą dieną po jo paskelbimo Europos Sąjungos oficialiajame leidinyje arba vėlesnę jame nurodytą dieną. Jis nedaro poveikio jau galiojančių deleguotųjų aktų galiojimui.	*Direktyvos straipsnio į nacionalinę teisę perkelti nereikia*	
4. Prieš priimdama deleguotąjį aktą Komisija konsultuojasi su kiekvienos valstybės narės paskirtais ekspertais vadovaudamasi 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros nustatytais principais.	*Direktyvos straipsnio į nacionalinę teisę perkelti nereikia*	
5. Apie priimtą deleguotąjį aktą Komisija nedelsdama vienu metu praneša Europos Parlamentui ir Tarybai.	*Direktyvos straipsnio į nacionalinę teisę perkelti nereikia*	

6. Pagal 24 straipsnio 2 dalį priimtas deleguotasis aktas įsigalioja tik tuo atveju, jeigu per du mėnesius nuo pranešimo Europos Parlamentui ir Tarybai apie šį aktą dienos nei Europos Parlamentas, nei Taryba nepareiškia prieštaravimų arba jeigu dar nepasibaigus šiam laikotarpiui ir Europos Parlamentas, ir Taryba praneša Komisijai, kad prieštaravimų nereikš. Europos Parlamento arba Tarybos iniciatyva šis laikotarpis pratęsiamas dviem mėnesiais.	*Direktyvos straipsnio į nacionalinę teisę perkelti nereikia*	
39 straipsnis. Komiteto procedūra		
1. Komisijai padeda komitetas. Tas komitetas – tai komitetas, kaip tai suprantama Reglamente (ES) Nr. 182/2011. 2. Kai daroma nuoroda į šią dalį, taikomas Reglamento (ES) Nr. 182/2011 5 straipsnis. 3. Kai komiteto nuomonei gauti būtina rašytinė procedūra, tokia procedūra laikoma baigta be rezultato, jei per nuomonei pateikti nustatytą laikotarpį taip nusprendžia komiteto pirmininkas arba to prašo komiteto narys.	*Direktyvos straipsnio į nacionalinę teisę perkelti nereikia*	
40 straipsnis. Peržiūra Komisija ne vėliau kaip 2027 m. spalio 17 d. peržiūri šios direktyvos taikymą ir teikia ataskaitą Europos Parlamentui ir Tarybai. Ataskaitoje visų pirma įvertinama susijusių subjektų dydžio ir I ir II prieduose nurodytų sektorių, subsektorių ir subjektų rūšių svarba ekonomikos ir visuomenės veikimui kibernetinio saugumo atžvilgiu. Tuo tikslu ir siekiant tolesnės pažangos vykdant strateginį ir operatyvinį bendradarbiavimą, Komisija atsižvelgia į Bendradarbiavimo grupės ir CSIRT tinklo ataskaitas apie patirtį, įgytą strateginiu ir operatyviniu lygmenimis. Kai būtina, prie ataskaitos pridedamas pasiūlymas dėl teisėkūros procedūra priimamo akto.	*Direktyvos straipsnio į nacionalinę teisę perkelti nereikia*	
41 straipsnis. Perkėlimas į nacionalinės teisės aktus		
1. Valstybės narės ne vėliau kaip 2024 m. spalio 17 d., priima ir paskelbia nuostatas, būtinas, kad būtų laikomasi šios direktyvos. Apie tai jos nedelsdamos praneša Komisijai. Tas nuostatas jos taiko nuo 2024 m. spalio 18 d.	**KSĮ projektas** **Kibernetinio saugumo įstatymo 3 priedas** **ĮGYVENDINAMI EUROPOS SĄJUNGOS TEISĖS AKTAI** **1. 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir**	Visiškas

2. Valstybės narės, priimdamos 1 dalyje nurodytas nuostatas, daro jose nuorodą į šią direktyvą arba tokia nuoroda daroma jas oficialiai skelbiant. Nuorodos darymo tvarką nustato valstybės narės.	**informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013.** **2. 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/887, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas.** **3. 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148.“** **2 straipsnis. Įstatymo įsigaliojimas, įgyvendinimas ir taikymas** **1. Šis įstatymas, išskyrus šio įstatymo 2 dalį, įsigalioja 2024 m. spalio 18 d.** **2. Lietuvos Respublikos Vyriausybė, krašto apsaugos ministras, Nacionalinio kibernetinio saugumo centro direktorius iki 2024 m. spalio 17 d. priima šio įstatymo įgyvendinamuosius teisės aktus.** **3. Nacionalinis kibernetinio saugumo centras iki 2025 m. balandžio 17 d. identifikuoja šio įstatymo 1 ir 2 prieduose nurodytuose sektoriuose veikiančius kibernetinio saugumo subjektus, atitinkančius šiuo įstatymu nauja redakcija išdėstyto Kibernetinio saugumo įstatymo 11 straipsnyje nustatytus reikalavimus, ir juos įtraukia į Kibernetinio saugumo subjektų registrą.** **4. Subjektai, kurie iki šio įstatymo įsigaliojimo buvo įtraukti į Vyriausybės patvirtintą ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašą, iki 2025 m. balandžio 17 d. privalo toliau užtikrinti jų valdomų tinklų ir informacinių sistemų atitiktį iki šio įstatymo įsigaliojimo galiojusiems Lietuvos Respublikos kibernetinio saugumo įstatymo 11 straipsnio 1 dalies 1 punkte nurodytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams, taikomiems kibernetinio saugumo subjektams.** **5. Subjektai, kurie iki šio įstatymo įsigaliojimo buvo įtraukti į Vyriausybės patvirtintą ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašą, įtraukti į Kibernetinio saugumo subjektų registrą, privalo toliau užtikrinti jų valdomų tinklų ir informacinių sistemų atitiktį iki šio įstatymo įsigaliojimo galiojusiems Kibernetinio saugumo įstatymo 11 straipsnio 1 dalies 1 punkte nurodytiems kibernetinio saugumo reikalavimams, taikomiems kibernetinio saugumo subjektams, tol, kol atsiras pareiga užtikrinti jų valdomų tinklų ir informacinių sistemų atitiktį šiuo įstatymu nauja redakcija išdėstyto**	

	Lietuvos Respublikos kibernetinio saugumo įstatymo 14 straipsnio 1 dalyje nurodytoms kibernetinio saugumo rizikos valdymo priemonėms. **6. Saugos įgaliotiniams, kuriems iki šio įstatymo įsigaliojimo buvo taikomos Kibernetinio saugumo įstatymo 22 straipsnio nuostatos dėl saugos įgaliotinio skyrimo ir atitikimo reikalavimams, toliau savo pareigas vykdo šiuo įstatymu nauja redakcija išdėstyto Lietuvos Respublikos kibernetinio saugumo įstatymo 15 straipsnio nustatyta tvarka. Šioje dalyje nurodytiems saugos įgaliotiniams šiuo įstatymu nauja redakcija išdėstyto Lietuvos Respublikos kibernetinio saugumo įstatymo 15 straipsnio 5 dalies 3punkto reikalavimai netaikomi pirmus 2 metus nuo šio įstatymo įsigaliojimo.** **7. Nacionalinis kibernetinio saugumo centas šio straipsnio 3 ir 4 dalyje nurodytais atvejais atlieka ryšių ir informacinių sistemų atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams, taikomiems kibernetinio saugumo subjektams, priežiūrą ir turi iki šio įstatymo įsigaliojimo galiojusiuose Kibernetinio saugumo įstatymo 8 straipsnio 2 dalies 1, 2, 4 ir 5 punktuose nurodytus įgaliojimus.** **8. Nacionalinis kibernetinio saugumo centras šio straipsnio 4 ir 5 dalyje nurodytais atvejais nustatęs iki šio įstatymo įsigaliojimo galiojusiame Kibernetinio saugumo įstatymo 11 straipsnio 1 dalies 1 punkte nurodytų organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, pažeidimų, taiko iki šio įstatymo įsigaliojimo galiojusias Lietuvos Respublikos administracinių nusižengimų kodekso 480 straipsnio 4 ir 5 dalies nuostatas.9. Vadovaujantis iki šio įstatymo įsigaliojimo galiojusio Kibernetinio saugumo įstatymu pradėtos procedūros, tęsiamos ir baigiamos vadovaujantis iki šio įstatymo įsigaliojimo galiojusiomis Kibernetinio saugumo įstatymo ir jį įgyvendinančių teisės aktų nuostatomis.** **10. Kituose teisės aktuose vartojama sąvoka „ryšių ir informacinė sistema“ atitinka šiame įstatyme vartojamą sąvoką „tinklų ir informacinė sistema“**	
42 straipsnis. Reglamento (ES) Nr. 910/2014 dalinis pakeitimas		
Reglamento (ES) Nr. 910/2014 19 straipsnis išbraukiamas nuo 2024 m. spalio 18 d.	**Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymo Nr. XIII-1120 4 straipsnio pakeitimo įstatymo projektas**	Visiškas
43 straipsnis. Direktyvos (ES) 2018/1972 dalinis pakeitimas		

<table>
<tr><td>Direktyvos (ES) 2018/1972 40 ir 41 straipsniai išbraukiami nuo 2024 m. spalio 18 d.</td><td>Lietuvos Respublikos elektroninių ryšių įstatymo Nr. IX-2135 3, 8, 36, 45, 51, 74, 82 ir 98 straipsnių pakeitimo įstatymo projektas</td><td>Visiškas</td></tr>
<tr><td>44 straipsnis. Panaikinimas
Direktyva (ES) 2016/1148 panaikinama nuo 2024 m. spalio 18 d. Nuorodos į panaikintą direktyvą laikomos nuorodomis į šią direktyvą ir skaitomos pagal III priede pateiktą atitikties lentelę.</td><td>Direktyvos straipsnio į nacionalinę teisę perkelti nereikia</td><td></td></tr>
<tr><td>45 straipsnis. Įsigaliojimas
Ši direktyva įsigalioja dvidešimtą dieną po jos paskelbimo Europos Sąjungos oficialiajame leidinyje.</td><td>Direktyvos straipsnio į nacionalinę teisę perkelti nereikia</td><td></td></tr>
<tr><td>46 straipsnis. Adresatai
Ši direktyva skirta valstybėms narėms.</td><td>Direktyvos straipsnio į nacionalinę teisę perkelti nereikia</td><td></td></tr>
<tr><td>I PRIEDAS. YPATINGOS SVARBOS SEKTORIAI</td><td></td><td></td></tr>
<tr><td>1. Energetika
a) Elektra
— Elektros energijos įmonės, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2019/944 (1)2 straipsnio 57 punkte, vykdančios „tiekimo“ funkciją, kaip apibrėžta tos direktyvos 2 straipsnio 12 punkte
— Skirstymo sistemos operatoriai, kaip apibrėžta Direktyvos (ES) 2019/944 2 straipsnio 29 punkte
— Perdavimo sistemos operatoriai, kaip apibrėžta Direktyvos (ES) 2019/944 2 straipsnio 35 punkte
— Gamintojai, kaip apibrėžta Direktyvos (ES) 2019/944 2 straipsnio 38 punkte
— Paskirtieji elektros energijos rinkos operatoriai, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2019/943 (2) 2 straipsnio 8 punkte
— Elektros energijos rinkos dalyviai, kaip apibrėžta Reglamento (ES) 2019/943 2 straipsnio 25 punkte, teikiantys telkimo, reguliavimo apkrovos arba energijos kaupimo paslaugas, nurodytas Direktyvos (ES) 2019/944 2 straipsnio 18, 20 ir 59 punktuose
— Įkrovimo prieigos operatoriui, atsakingi už įkrovimo prieigos, kuri naudojama įkrovimo paslaugai galutiniams</td><td>KSĮ projektas
Lietuvos Respublikos kibernetinio saugumo įstatymo 1 priedas YPATINGOS SVARBOS SEKTORIAI
<table>
<tr><th>Sektorius</th><th>Subsektorius</th><th>Subjekto rūšis</th><th>Institucija, atsakinga už identifikavimą</th></tr>
<tr><td rowspan="3">1. Energetika</td><td rowspan="3">1.1. Elektra</td><td>1.1.1. Elektros energetikos įmonės, vykdančios elektros energijos tiekimo funkciją.</td><td>Lietuvos Respublikos energetikos ministerija</td></tr>
<tr><td>1.1.2. Elektros energijos skirstomųjų tinklų operatorius.</td><td>Energetikos ministerija</td></tr>
<tr><td>1.1.3. Elektros energijos perdavimo sistemos operatorius.</td><td>Energetikos ministerija</td></tr>
</table></td><td>Visiškas</td></tr>
</table>

naudotojams teikti, taip pat ir judumo paslaugų teikėjo vardu bei jo pavedimu, valdymą ir eksploatavimą b) Centralizuotas šilumos ir vėsumos tiekimas — Centralizuoto šilumos tiekimo arba centralizuoto vėsumos tiekimo, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2018/2001 (3)2 straipsnio 19 punkte, operatoriai c) Nafta — Naftotiekių operatoriai — Naftos gamybos, perdirbimo ir apdorojimo įrenginių, laikymo ir perdavimo operatoriai — Centrinės atsargų saugyklos, kaip apibrėžta Tarybos direktyvos 2009/119/EB (4)2 straipsnio f punkte d) Dujos — Tiekimo įmonės, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2009/73/EB (5)2 straipsnio 8 punkte — Skirstymo sistemos operatoriai, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 6 punkte — Perdavimo sistemos operatoriai, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 4 punkte — Laikymo sistemų operatoriai, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 10 punkte — SGD sistemos operatoriai, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 12 punkte — Gamtinių dujų įmonės, kaip apibrėžta Direktyvos 2009/73/EB 2 straipsnio 1 punkte — Gamtinių dujų perdirbimo ir apdorojimo įrenginių operatoriai e) Vandenilis — Vandenilio gamybos, laikymo ir perdavimo operatoriai			**1.1.4. Elektros energijos gamintojas.**	**Energetikos ministerija**	
			1.1.5. Paskirtieji elektros energijos rinkos operatoriai, kaip apibrėžta 2019 m. birželio 5 d. Europos Parlamento ir Tarybos reglamento (ES) 2019/943 dėl elektros energijos vidaus rinkos 2 straipsnio 8 punkte.	**Energetikos ministerija**	
			1.1.6. Elektros energijos rinkos dalyviai, kaip apibrėžta 2019 m. birželio 5 d. Europos Parlamento ir Tarybos reglamento (ES) 2019/(ES) 2019/943 dėl elektros energijos vidaus rinkos 2 straipsnio 25 punkte, teikiantys elektros energijos paklausos telkimo, energijos kaupimo paslaugas, , bei teikiantys elektros energijos reguliavimo apkrovos paslaugas.	**Energetikos ministerija**	
			1.1.7. Elektromobilių įkrovimo prieigos operatorius.	**Energetikos ministerija**	
		1.2. Centralizuotas šilumos ir vėsumos tiekimas	**1.2.1. Centralizuoto šilumos ar vėsumos energijos tiekimo operatoriai.**	**Energetikos ministerija**	
		1.3. Nafta	**1.3.1. Naftotiekį valdanti įmonė.**	**Energetikos ministerija**	
			1.3.2. Naftos gamybos įmonė.	**Energetikos ministerija**	
2. Transportas a) Oro transportas — Oro vežėjai, kaip apibrėžta Reglamento (EB) Nr. 300/2008 3 straipsnio 4 punkte, naudojami komerciniais tikslais					

— Oro uosto valdymo organai, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2009/12/EB (6)2 straipsnio 2 punkte, oro uostai, kaip apibrėžta tos direktyvos 2 straipsnio 1 punkte, įskaitant Europos Parlamento ir Tarybos reglamento (ES) Nr. 1315/2013 (7)II priedo 2 skirsnyje išvardytus pagrindinius oro uostus, ir subjektai, eksploatuojantys oro uostuose esančius pagalbinius įrenginius — Skrydžių valdymo operatoriai, teikiantys skrydžių valdymo (ATC) paslaugas, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (EB) Nr. 549/2004 (8)2 straipsnio 1 punkte b) Geležinkelių transportas — Infrastruktūros valdytojai, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2012/34/ES (9)3 straipsnio 2 punkte — Geležinkelio įmonės, kaip apibrėžta Direktyvos 2012/34/ES 3 straipsnio 1 punkte, įskaitant paslaugų įrenginių operatorius, kaip apibrėžta tos direktyvos 3 straipsnio 12 punkte c) Vandens transportas — Vidaus vandenų, jūrų ir priekrantės keleivinio ir krovininio vandens transporto bendrovės, kaip apibrėžta jūrų transporto atžvilgiu Europos Parlamento ir Tarybos reglamento (EB) Nr. 725/2004 (10) I priede, neįskaitant tų bendrovių eksploatuojamų atskirų laivų — Uostų, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2005/65/EB (11)3 straipsnio 1 punkte, įskaitant jų uosto įrenginius, kaip apibrėžta Reglamento (EB) Nr. 725/2004 2 straipsnio 11 punkte, direkcijos ir subjektai, eksploatuojantys uostuose esančias įmones ir įrenginius — Laivų eismo tarnybų (LET), kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2002/59/EB (12) 3 straipsnio o punkte, operatoriai d) Kelių transportas			**Naftą importuojanti įmonė, naftą įvežanti įmonė, naftos atsargas kaupianti įmonė, naftos atsargas tvarkanti įmonė.**		
			1.3.3.Centrinė naftos produktus ir naftos atsargas kaupianti ir tvarkanti organizacija.	**Energetikos ministerija**	
		1.4. Dujos	**1.4.1. Gamtinių dujų tiekimo įmonė.**	**Energetikos ministerija**	
			1.4.2. Gamtinių dujų skirstymo sistemos operatorius.	**Energetikos ministerija**	
			1.4.3. Gamtinių dujų perdavimo sistemos operatorius.	**Energetikos ministerija**	
			1.4.4. Gamtinių dujų laikymo sistemos operatorius.	**Energetikos ministerija**	
			1.4.5. Suskystintų gamtinių dujų sistemos operatorius.	**Energetikos ministerija**	
			1.4.6. Gamtinių dujų įmonė.	**Energetikos ministerija**	
			1.4.7. Gamtinių dujų perdirbimo ir apdorojimo įrenginių operatoriai.	**Energetikos ministerija**	
		1.5. Vandenilis	**1.5.1. Vandenilio gamybos, laikymo ir perdavimo operatoriai.**	**Energetikos ministerija**	
	2. Transportas	**2.1. Oro transportas**	**2.1.1. Oro vežėjai, kaip apibrėžta 2008 m. kovo 11 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 300/2008 dėl civilinės aviacijos saugumo bendrųjų taisyklių ir panaikinančio Reglamentą (EB)**	**Lietuvos Respublikos susisiekim**	

— Kelių direkcijos, kaip apibrėžta Komisijos deleguotojo reglamento (ES) 2015/962 (13) 2 straipsnio 12 punkte, atsakingos už eismo valdymo kontrolę, išskyrus viešuosius subjektus, kuriems eismo valdymo arba intelektinių transporto sistemų operatoriaus veikla yra tik neesminė jų bendrosios veiklos dalis — Intelektinių transporto sistemų, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2010/40/ES (14) 4 straipsnio 1 punkte, operatoriai			**Nr. 2320/2002 3 straipsnio 4 punkte, naudojami komerciniais tikslais.**	**o ministerija**
			2.1.2. Oro uostas, įskaitant 2013 m. gruodžio 11 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 1315/2013 dėl Sąjungos transeuropinio transporto tinklo plėtros gairių, kuriuo panaikinamas Sprendimas Nr. 661/2010/ES, II priedo 2 skirsnyje išvardytus pagrindinius oro uostus, ir oro uostą valdančios įmonės vadovas. **Subjektai, eksploatuojantys oro uostuose esančius pagalbinius įrenginius.**	**Susisiekimo ministerija**
3. Bankininkystė Kredito įstaigos, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) Nr. 575/2013 (15)4 straipsnio 1 punkte				
4. Finansų rinkų infrastruktūros objektai — Prekybos vietų, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2014/65/ES (16)4 straipsnio 24 punkte, operatoriai — Pagrindinės sandorio šalys (PSŠ), kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) Nr. 648/2012 (17) 2 straipsnio 1 punkte			**2.1.3. Skrydžių valdymo operatoriai, teikiantys skrydžių valdymo paslaugas, kaip apibrėžta 2004 m. kovo 10 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 549/2004, nustatančio bendro Europos dangaus sukūrimo pagrindą, 2 straipsnio 1 punkte.**	**Susisiekimo ministerija**
5. Sveikatos priežiūra — Sveikatos priežiūros paslaugų teikėjai, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2011/24/ES (18)3 straipsnio g punkte — ES etaloninės laboratorijos, nurodytos Europos Parlamento ir Tarybos reglamento (ES) 2022/2371 (19) 15 straipsnyje — Subjektai, vykdantys vaistų, apibrėžtų Europos Parlamento ir Tarybos direktyvos 2001/83/EB (20)1 straipsnio 2 punkte, mokslinių tyrimų ir kūrimo veiklą — Subjektai, gaminantys pagrindinius farmacijos produktus ir farmacijos preparatus, nurodytus NACE 2 red. C skirsnio 21 skyriuje — Subjektai, gaminantys medicinos priemones, kurios laikomos ypatingos svarbos ekstremaliosios visuomenės sveikatos situacijos atveju (ypatingos svarbos medicinos		**2.2. Geležinkelių transportas**	**2.2.1. Geležinkelių infrastruktūros valdytojas.**	**Susisiekimo ministerija**
			2.2.2. Geležinkelio įmonė (vežėjas).	**Susisiekimo ministerija**
			2.2.3. Geležinkelių paslaugų įrenginio operatorius.	**Susisiekimo ministerija**
		2.3. Vandens transportas	**2.3.1. Vidaus vandenų, jūrų ir priekrantės keleivinio ir krovininio vandens transporto bendrovės, kaip apibrėžta jūrų transporto atžvilgiu 2004 m. kovo 31 d. Europos**	**Susisiekimo ministerija**

priemonių ekstremaliosios visuomenės sveikatos situacijos atveju sąrašas), kaip tai suprantama Europos Parlamento ir Tarybos reglamento (ES) 2022/123 (21) 22 straipsnyje			**Parlamento ir Tarybos reglamento (EB) Nr. 725/2004 dėl laivų ir uostų įrenginių apsaugos stiprinimo I priede, neįskaitant tų bendrovių eksploatuojamų atskirų laivų.**	
6. Geriamasis vanduo Žmonėms vartoti skirto vandens, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2020/2184 (22) 2 straipsnio 1 punkto a papunktyje, tiekėjai ir skirstytojai, išskyrus skirstytojus, kuriems žmonėms vartoti skirto vandens skirstymas yra neesminė jų bendrosios kitų prekių ir produktų paskirstymo veiklos dalis			**2.3.2. Uostus, , įskaitant jų uosto įrenginius, kaip apibrėžta 2004 m. kovo 31 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 725/2004 dėl laivų ir uostų įrenginių apsaugos stiprinimo 2 straipsnio 11 punkte, valdančios įmonės, bei subjektai, eksploatuojantys uostuose esančias įmones ir įrenginius.**	**Susisiekimo ministerija**
7. Nuotekos Miesto nuotekas, buitines nuotekas ir pramonines nuotekas, nurodytas Tarybos direktyvos 91/271/EEB (23) 2 straipsnio 1, 2 ir 3 punktuose, renkančios, šalinančios ar valančios įmonės, išskyrus įmones, kurioms miesto nuotekų, buitinių nuotekų ar pramoninių nuotekų rinkimas, šalinimas ar valymas yra neesminė jų bendrosios veiklos dalis			**2.3.3. Laivų eismo tarnybų operatoriai.**	**Susisiekimo ministerija**
		2.4. Kelių transportas	**2.4.1. Kelių direkcijos, kaip apibrėžta 2014 m. gruodžio 18 d. Komisijos deleguotojo (ES) Nr. 2015/962, kuriuo papildomos Europos Parlamento ir Tarybos direktyvos 2010/40/ES nuostatos, susijusios su visoje Europos Sąjungoje teikiamomis tikralaikės eismo informacijos paslaugomis, 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.**	**Susisiekimo ministerija**
8. Skaitmeninė infrastruktūra — Interneto duomenų srautų mainų taško teikėjai — DNS paslaugų teikėjai, išskyrus šakninio pavadinimo serverių operatorius — Aukščiausio lygio domenų vardų registrai — Debesijos kompiuterijos paslaugų teikėjai — Duomenų centrų paslaugų teikėjai — Turinio teikimo tinklo teikėjai — Patikimumo užtikrinimo paslaugų teikėjai — Viešųjų elektroninių ryšių tinklų teikėjai — Viešai prieinamų elektroninių ryšių paslaugų teikėjai			**2.4.2. Intelektinių transporto sistemų operatoriai.**	**Susisiekimo ministerija**
9. IRT paslaugų valdymas (verslas verslui) — Valdomų paslaugų teikėjai — Valdomų saugumo paslaugų teikėjai	**3. Bankininkystė**		**3.1.1. Kredito įstaigos, kaip apibrėžta 2013 m. birželio 26 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 575/2013 dėl**	**Lietuvos Respublik**
10. Viešasis administravimas — Centrinės valdžios viešojo administravimo subjektai, kaip valstybė narė apibrėžė pagal nacionalinę teisę				

— Regioninio lygmens viešojo administravimo subjektai, kaip valstybė narė apibrėžė pagal nacionalinę teisę			**prudencinių reikalavimų kredito įstaigoms ir investicinėms įmonėms ir kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 648/2012 4 straipsnio 1 punkte.**	**os finansų ministerija**	
11. Kosmosas Valstybėms narėms arba privačiosioms šalims priklausančios, jų valdomos ir eksploatuojamos antžeminės infrastruktūros operatoriai, kurie remia kosminių paslaugų teikimą, išskyrus viešųjų elektroninių ryšių tinklų teikėjus	**4. Finansų rinkų infrastruktūros objektai**		**4.1.1. Prekybos vietų operatoriai.**	**Finansų ministerija**	
			4.1.2. Pagrindinės sandorio šalys, kaip apibrėžta 2013 m. birželio 26 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 648/2012 dėl ne biržos išvestinių finansinių priemonių, pagrindinių sandorio šalių ir sandorių duomenų saugyklų 2 straipsnio 1 punkte.	**Finansų ministerija**	
	5. Sveikatos priežiūra		**5.1.1. Asmens sveikatos priežiūros įstaiga**	**Lietuvos Respublikos sveikatos apsaugos ministerija**	
			5.1.2. Europos Sąjungos etaloninės laboratorijos, nurodytos 2022 m. lapkričio 23 d. Europos Parlamento ir Tarybos reglamento (ES) 2022/2371 dėl didelių tarpvalstybinio pobūdžio grėsmių sveikatai, kuriuo panaikinamas Sprendimas Nr. 1082/2013/ES, 15 straipsnyje.	**Sveikatos apsaugos ministerija**	
			5.1.3. Subjektai, vykdantys vaistų (vaistinių preparatų), mokslinių tyrimų ir kūrimo veiklą.	**Sveikatos apsaugos ministerija**	

				5.1.4. Subjektai, gaminantys pagrindinius farmacijos produktus ir farmacijos preparatus, nurodytus Ekonominės veiklos rūšių klasifikatoriaus 2 redakcijos C skirsnio 21 skyriuje.	**Sveikatos apsaugos ministerija**	
				5.1.5. Subjektai, gaminantys medicinos priemones, kurios laikomos ypatingos svarbos ekstremaliosios visuomenės sveikatos situacijos atveju (ypatingos svarbos medicinos priemonių ekstremaliosios visuomenės sveikatos situacijos atveju sąrašas), kaip tai suprantama pagal 2022 m. sausio 25 d. Europos Parlamento ir Tarybos reglamento (ES) 2022/123 dėl didesnio Europos vaistų agentūros vaidmens pasirengimo vaistų ir medicinos priemonių krizei ir jos valdymo srityje 22 straipsnį.	**Sveikatos apsaugos ministerija**	
	6. Geriamasis vanduo		**6.1.1. Žmonėms vartoti skirto vandens tiekėjai ir skirstytojai, išskyrus skirstytojus, kuriems žmonėms vartoti skirto vandens skirstymas yra neesminė jų bendrosios kitų prekių ir produktų paskirstymo veiklos dalis.**	**Lietuvos Respublikos aplinkos ministerija**	
	7. Nuotekos		**7.1.1. Nuotekas renkančios, šalinančios ar valančios įmonės, išskyrus įmones, kurioms miesto nuotekų, buitinių nuotekų ar pramoninių nuotekų rinkimas, šalinimas ar valymas yra neesminė jų bendrosios veiklos dalis.**	**Aplinkos ministerija**	
	8. Skaitmeninė infrastruktūra		**8.1.1. Interneto duomenų srautų mainų taško teikėjai.**	**Susisiekimo ministerija**	
			8.1.2. Domenų vardų sistemos paslaugų teikėjai.	**Lietuvos Respublik**	

				os ekonomikos ir inovacijų ministerija	
			8.1.3. Aukščiausio lygio domenų vardų registro paslaugas teikiantys subjektai.	**Ekonomikos ir inovacijų ministerija**	
			8.1.4. Debesijos kompiuterijos paslaugų teikėjai.	**Ekonomikos ir inovacijų ministerija**	
			8.1.5. Duomenų centrų paslaugų teikėjai.	**Ekonomikos ir inovacijų ministerija**	
			8.1.6. Turinio teikimo tinklo teikėjai.	**Ekonomikos ir inovacijų ministerija**	
			8.1.7. Patikimumo užtikrinimo paslaugų teikėjai.	**Ekonomikos ir inovacijų ministerija**	
			8.1.8. Viešųjų elektroninių ryšių tinklų teikėjai.	**Susisiekimo ministerija**	
			8.1.9. Viešųjų elektroninių ryšių paslaugų teikėjai.	**Susisiekimo ministerija**	
		9. Informacinių ir		**9.1.1. Valdomų paslaugų teikėjai.**	**Ministerijos**	

	ryšių technologijų paslaugų valdymas (verslas verslui)		**9.1.2. Valdomų saugumo paslaugų teikėjai.**	**Ministerijos**	
	10. Viešasis administravimas		**10.1.1. Valstybinio administravimo subjektai.**	**Lietuvos Respublikos vidaus reikalų ministerija**	
			10.1.2. Regioninio administravimo subjektai ir savivaldybių administravimo subjektai.	**Vidaus reikalų ministerija**	
	11. Kosmosas		**11.1.1. Lietuvos Respublikos įsteigtos arba privatiems subjektams priklausančios, jų valdomos ir eksploatuojamos antžeminės infrastruktūros operatoriai, kurie remia kosminių paslaugų teikimą, išskyrus viešųjų elektroninių ryšių tinklų teikėjus.**	**Ekonomikos ir inovacijų ministerija**	
II PRIEDAS. KITI ITIN SVARBŪS SEKTORIAI					
1. Pašto ir kurjerių paslaugos Pašto paslaugų teikėjai, kaip apibrėžta Direktyvos 97/67/EB 2 straipsnio 1a punkte, įskaitant kurjerių paslaugų teikėjus	**KSĮ projektas** **Lietuvos Respublikos kibernetinio saugumo įstatymo 2 priedas** **KITI ITIN SVARBŪS SEKTORIAI**				Visiškas
2. Atliekų tvarkymas Atliekas, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos 2008/98/EB (1) 3 straipsnio 9 punkte, tvarkančios įmonės, išskyrus įmones, kurių pagrindinė ekonominė veikla nėra atliekų tvarkymas	**Sektorius**	**Subsektorius**	**Subjekto rūšis**	**Institucija, atsakinga už subjektų identifikavimą**	
3. Cheminių medžiagų gamyba ir platinimas Chemines medžiagas gaminančios ir chemines medžiagas ar mišinius platinančios įmonės, kaip nurodyta Europos Parlamento					

ir Tarybos reglamento (EB) Nr. 1907/2006 (2) 3 straipsnio 9 ir 14 punktuose, ir gaminius, kaip apibrėžta to reglamento 3 straipsnio 3 punkte, iš tų medžiagų ar mišinių gaminančios įmonės	**1. Pašto paslaugos**		**1.1.1. Pašto paslaugos teikėjai.**	**Lietuvos Respublikos susisiekimo ministerija**	
4. Maisto gamyba, perdirbimas ir platinimas Maisto verslo įmonės, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (EB) Nr. 178/2002 (3) 3 straipsnio 2 punkte, vykdančios didmeninio platinimo ir pramoninės gamybos bei perdirbimo veiklą	**2. Atliekų tvarkymas**		**2.1.1. Atliekų tvarkymo paslaugų teikėjai, išskyrus paslaugų teikėjus, kurių pagrindinė ekonominė veikla nėra atliekų tvarkymas.**	**Lietuvos Respublikos aplinkos ministerija**	
5. Gamyba a) Medicinos priemonių ir in vitro diagnostikos medicinos priemonių gamyba Medicinos priemones, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2017/745 (4) 2 straipsnio 1 punkte, gaminantys subjektai, ir in vitro diagnostikos medicinos priemones, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES) 2017/746 (5) 2 straipsnio 2 punkte, gaminantys subjektai, išskyrus šios direktyvos I priedo 5 punkto penktoje įtraukoje nurodytas medicinos priemones gaminančius subjektus. b) Kompiuterinių, elektroninių ir optinių gaminių gamyba Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 26 skyriuje c) Elektros įrangos gamyba Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 27 skyriuje d) Niekur kitur nepriskirtų mašinų ir įrangos gamyba Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 28 skyriuje e) Motorinių transporto priemonių, priekabų ir puspriekabių gamyba Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 29 skyriuje f) Kitos transporto įrangos gamyba Įmonės, vykdančios bet kurią ekonominę veiklą, nurodytą NACE 2 red. C skirsnio 30 skyriuje	**3. Cheminių medžiagų gamyba ir platinimas**		**3.1.1. Chemines medžiagas gaminančios ir chemines medžiagas ar mišinius platinančios įmonės, kaip nurodyta 2006 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 1907/2006 dėl cheminių medžiagų registracijos, įvertinimo, autorizacijos ir apribojimų (REACH), įsteigiančio Europos cheminių medžiagų agentūrą, iš dalies keičiančio Direktyvą 1999/45/EB bei panaikinančio 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, 3 straipsnio 9 ir 14 punktuose, ir gaminius, kaip apibrėžta to paties reglamento 3 straipsnio 3 punkte, iš tų medžiagų ar mišinių gaminančios įmonės.**	**Aplinkos ministerija**	
6. Skaitmeninių paslaugų teikėjai	**4. Maisto gamyba, perdirbi**		**4.1.1. Maisto verslo įmonės, kaip apibrėžta 2002 m. sausio 28 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 178/2002, nustatančio maistui skirtų**	**Lietuvos Respublikos žemės**	

— Elektroninių prekyviečių teikėjai — Paieškos sistemų teikėjai — Socialinių tinklų paslaugų platformos teikėjai 7. Moksliniai tyrimai Mokslinių tyrimų organizacijos	**mas ir platinimas**		**teisės aktų bendruosius principus ir reikalavimus, įsteigiančio Europos maisto saugos tarnybą ir nustatančio su maisto saugos klausimais susijusias procedūras, 3 straipsnio 2 punkte, vykdančios didmeninio platinimo ir pramoninės gamybos bei perdirbimo veiklą.**	**ūkio ministerija**	
	5. Gamyba	**5.1. Medicinos priemonių ir *in vitro* diagnostikos medicinos priemonių gamyba**	**5.1.1. Medicinos priemones, kaip apibrėžta 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos reglamento (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, 2 straipsnio 1 punkte, gaminantys subjektai ir *in vitro* diagnostikos medicinos priemones, kaip apibrėžta 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos reglamento (ES) 2017/746 dėl *in vitro* diagnostikos medicinos priemonių, kuriuo panaikinama Direktyva 98/79/EB ir Komisijos sprendimas 2010/227/ES, 2 straipsnio 2 punkte, gaminantys subjektai, išskyrus šios įstatymo I priedo 5.1.5 papunktyje nurodytas medicinos priemones gaminančius subjektus.**	**Lietuvos Respublikos sveikatos apsaugos ministerija**	
		5.2. Kompiuterinių, elektroninių ir optinių gaminių gamyba	**5.2.1. Subjektai, vykdantys bet kurią ekonominę veiklą, nurodytą Ekonominės veiklos rūšių klasifikatoriaus 2 redakcijos C skirsnio 26 skyriuje.**	**Lietuvos Respublikos ekonomikos ir inovacijų ministerija**	

		5.3. Elektros įrangos gamyba	**5.3.1. Subjektai, vykdantys bet kurią ekonominę veiklą, nurodytą Ekonominės veiklos rūšių klasifikatoriaus 2 redakcijos C skirsnio 27 skyriuje.**	**Lietuvos Respublikos energetikos ministerija**	
		5.4. Niekur kitur nepriskirtų mašinų ir įrangos gamyba	**5.4.1. Subjektai, vykdantys bet kurią ekonominę veiklą, nurodytą Ekonominės veiklos rūšių klasifikatoriaus 2 redakcijos C skirsnio 28 skyriuje.**	**Ministerijos**	
		5.5. Motorinių transporto priemonių, priekabų ir puspriekabių gamyba	**5.5.1. Subjektai, vykdantys bet kurią ekonominę veiklą, nurodytą Ekonominės veiklos rūšių klasifikatoriaus 2 redakcijos C skirsnio 29 skyriuje.**	**Susisiekimo ministerija**	
		5.6. Kitos transporto įrangos gamyba	**5.6.1. Subjektai, vykdantys bet kurią ekonominę veiklą, nurodytą Ekonominės veiklos rūšių klasifikatoriaus 2 redakcijos C skirsnio 30 skyriuje.**	**Susisiekimo ministerija**	
	6. Informacinės visuomenės paslaugos		**6.1.1. Elektroninių prekyviečių teikėjai.**	**Ekonomikos ir inovacijų ministerija**	
			6.1.2. Paieškos sistemų teikėjai.	**Ekonomikos ir inovacijų ministerija**	
			6.1.3. Socialinių tinklų paslaugų platformos teikėjai.	**Ekonomikos ir**	

				inovacijų ministerija	
			6.1.4. Subjektas, teikiantis kitas elektroninės informacijos prieglobos paslaugas	**Ekonomikos ir inovacijų ministerija**	
	7. Moksliniai tyrimai		**7.1.1. Mokslinius tyrimus vykdantys subjektai.**	**Lietuvos Respublikos švietimo, mokslo ir sporto ministerija**	
III PRIEDAS. ATITIKTIES LENTELĖ	*Direktyvos nuostatos į nacionalinę teisę perkelti nereikia, nes dėl šios nuostatos Lietuvos Respublika neturi imtis jokių veiksmų.*				

_____