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 įstatymas (toliau – KSĮ)** **2. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ projektas (toliau – Nutarimo projektas)**	**Direktyvos (kito ES teisės akto) perkėlimo (įgyvendinimo lygis (visiškas, dalinis)**
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: <...> e) parengties, reagavimo į incidentus ir veiklos po incidento atstatymo priemonių, įskaitant viešojo ir privačiojo sektorių bendradarbiavimą, nustatymą;	**Nacionalinis kibernetinių incidentų valdymo planas, tvirtinamas Nutarimo projektu.** **3. Kibernetinių incidentų valdymo organizavimą kibernetinio saugumo subjekto lygmeniu užtikrina kibernetinio saugumo subjektas. Kibernetinių incidentų valdymo organizavimas užtikrinamas vykdant šiuo Vyriausybės nutarimu tvirtinamo Kibernetinio saugumo reikalavimų aprašo 25 ir 26 punktuose numatytas funkcijas ir kibernetinio saugumo subjekto vadovui ar jo įgaliotam asmeniui paskiriant šias funkcijas vykdančius asmenis (toliau – Saugumo operacijų centras). Kibernetinio saugumo subjektas užtikrina, kad Saugumo operacijų centro funkcijos nebūtų pavedamos kibernetinio saugumo subjekto arba paslaugų teikėjo darbuotojui, atsakingam už tinkamą to kibernetinio saugumo subjekto tinklų ir (ar) informacinių sistemų veiklą.** **4. Kibernetinio saugumo subjektas kibernetinių incidentų valdymą organizuoja pagal kibernetinio saugumo subjekto patvirtintą kibernetinių incidentų valdymo planą. Šis planas privalo apimti Tipinio kibernetinių incidentų valdymo proceso schemoje (Plano 1 priedas) ir Tipiniame kibernetinių incidentų valdymo proceso aprašyme (Plano 2 priedas) numatytus dalyvius, etapus, veiksmus, terminus ir rezultatus.** **5. Kibernetinis incidentas laikomas suvaldytu, kai yra atkurtos kibernetinio saugumo subjektų tinklų ir informacinėmis sistemomis teikiamos paslaugos.** **6. Nacionaliniu lygmeniu kibernetinių incidentų valdymą pagal Nacionalinio kibernetinių incidentų valdymo proceso schemą (Plano 3 priedas) ir aprašymą**	Visiškas

	(Plano 4 priedas) užtikrina Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC). **7. NKSC, pagal kibernetinio saugumo subjekto prašymą spręsdamas dėl resursų skyrimo dideliam kibernetiniam incidentui valdyti, sprendimą priima įvertinęs tikimybę, kad didelis kibernetinis incidentas taps ekstremaliuoju įvykiu. Prioritetas skiriamas kibernetiniams incidentams, kurių padariniai labiausiai atitinka arba daugiausiai viršija Vyriausybės nustatytus ekstremaliojo įvykio kriterijus.** **8. Įvykus arba kilus grėsmei įvykti dideliam kibernetiniam incidentui, atitinkančiam ekstremaliojo įvykio kriterijus, NKSC apie tai informuoja Lietuvos Respublikos Vyriausybės kanceliarijos Nacionalinį krizių valdymo centrą (toliau – NKVC).** **<...>** **10. Kibernetinio saugumo subjekto Saugumo operacijų centras apie kibernetinius incidentus informuoja NKSC, juos registruodamas Kibernetinio saugumo informacinės sistemos posistemyje – Nacionalinėje kibernetinių incidentų valdymo platformoje (toliau – Platforma).** **11. Kibernetinio saugumo subjekto Saugumo operacijų centras, dėl kibernetinio incidento neturintis galimybės apie kibernetinius incidentus informuoti automatizuotu būdu per Platformą, NKSC informuoja užpildydamas formą Platformoje, NKSC interneto svetainėje, NKSC nurodytu elektroninio pašto adresu arba telefonu.** **12. Kibernetinio saugumo subjekto Saugumo operacijų centras apie didelį kibernetinį incidentą NKSC informuoja Kibernetinio saugumo įstatymo 18 straipsnio 4 dalyje nustatytais terminais pateikdamas toje pačioje dalyje nurodytą informaciją. Kibernetinio saugumo subjekto Saugumo operacijų centras turi teisę teikti ir kitą, Kibernetinio saugumo įstatymo 18 straipsnio 4 dalyje nenurodytą, tačiau dideliam kibernetiniam incidentui suvaldyti ar tirti reikšmingą informaciją.** **<...>** **17. Asmenys, neturintys pareigos NKSC pranešti apie kibernetinius incidentus, apie kibernetinius incidentus, kibernetines grėsmes, vos neįvykusius kibernetinius incidentus ir (ar) taikytas kibernetinių incidentų valdymo priemones NKSC savanoriškai praneša:**	

	17.1. kibernetinio saugumo subjekto Saugumo operacijų centras – tokia pat tvarka, kaip ir apie kibernetinius incidentus; **17.2. asmenys, kurie nėra kibernetinio saugumo subjektai – NKSC interneto svetainėje skelbiamais būdais.**	
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;	**Kibernetinio saugumo reikalavimų aprašas, tvirtinamas Nutarimo projektu.** **Šeštasis skirsnis. Tiekimo grandinės saugumas** **32. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi nustatyti tiekimo grandinės saugumo valdymo tvarką, taikomą paslaugų, darbų ar įrangos pirkimams, susijusiems su tinklų ir informacinių sistemų projektavimu, kūrimu, diegimu, naudojimu, priežiūra, modernizavimu ir (ar) kibernetinio saugumo užtikrinimu, siekiant mažinti galimas kilti rizikas tinklų ir informacinėms sistemoms.** **33. Kibernetinio saugumo subjektas, nustatydamas tiekimo grandinės saugumo valdymo tvarką, turi numatyti tinklų ir informacinių sistemų tiekėjų atrankos kriterijus, apimančius:** **33.1. tiekėjo atitiktį Apraše nustatytiems kibernetinio saugumo reikalavimams;** **33.2. kokybės reikalavimus tinklų ir informacinių sistemų produktams, paslaugoms;** **33.3. prieigų valdymą, įskaitant prieigų laikotarpio ribojimą.** **34. Kibernetinio saugumo subjektas sutartyse su tiekėjais (įskaitant subtiekėjus), kiek tai susiję su teikiamomis paslaugomis, turi numatyti:** **34.1. tiekėjo atitikties šiam Aprašui reikalavimus;** **34.2. tiekėjo personalui reikalingus įgūdžius ir (ar) mokymus, ir (ar) sertifikatus, ir (ar) kvalifikaciją;** **34.3. tiekėjo pareigą pranešti kibernetinio saugumo subjektui apie visus didelius ir (ar) kitus incidentus, susijusius su kibernetinio saugumo subjekto tinklų ir informacinėmis sistemomis, kai tik tiekėjas sužino apie incidentą, ir pateikti kibernetinio saugumo subjektui kibernetinio incidento tyrimo ataskaitą;** **34.4. teisę kibernetinio saugumo subjektui arba jo įgaliotiems paslaugų teikėjams atlikti tiekėjo atitikties Aprašui auditą (įskaitant neplaninį) ir tiekėjo pareigą sudaryti sąlygas tokiam auditui atlikti sutarties vykdymo laikotarpiu ar įvykus dideliam incidentui;**	Visiškas

	34.5. pareigą užtikrinti spragų, keliančių riziką kibernetinio saugumo subjekto tinklams ir informacinėms sistemoms, valdymą; **34.6. konfidencialumo ir duomenų neatskleidimo įsipareigojimus;** **34.7. paslaugų teikimo lygmenis (angl. Service Level Agreement, SLA);** **34.8. apibrėžti tiekėjų prieigos (loginės ir fizinės) prie tinklų ir informacinės sistemos lygius ir sąlygas;** **34.9. numatyti reikalavimus, keliamus tiekėjo patalpoms, įrangai, tinklų ir informacinių sistemų priežiūrai, informacijos perdavimui tinklais;** **34.10. numatyti tiekėjo ir kibernetinio saugumo subjekto teises ir pareigas.** **35. Kibernetinio saugumo subjektas, tvirtindamas tiekimo grandinės saugumo valdymo tvarką, turi numatyti tinklų ir informacinių sistemų paslaugų teikėjų rizikos vertinimo reikalavimus.** **36. Esminis kibernetinio saugumo subjektas su interneto paslaugos, jei duomenų perdavimo paslauga yra esminė paslaugai teikti, teikėju turi būti sudaręs sutartį (-is), kurioje (-iose) būtų numatyta:** **36.1. reagavimas į kibernetinius incidentus įprastomis darbo valandomis;** **36.2. reagavimas į kibernetinius incidentus po darbo valandų;** **36.3. nepertraukiamas interneto paslaugos teikimas: 24 valandas per parą, 7 dienas per savaitę;** **36.4. paslaugos sutrikimų registravimas: 24 valandas per parą, 7 dienas per savaitę;** **36.5. apsaugos nuo tinklų ir informacinės sistemos trikdymo taikymas (angl. *Denial of Service*, DoS).** **37. Svarbus kibernetinio saugumo subjektas su interneto paslaugos, jei duomenų perdavimo paslauga yra esminė paslaugai teikti, teikėju turi būti sudaręs sutartį (-is), kurioje (-iose) turi būti numatyta:** **37.1. reagavimas į kibernetinius incidentus įprastomis darbo valandomis;** **37.2. nepertraukiamas paslaugos teikimas įprastomis darbo valandomis;** **37.3. paslaugos sutrikimų registravimas įprastomis darbo valandomis;** **37.4. apsaugos nuo tinklų ir informacinės sistemos trikdymo taikymas (DoS).** **38. Kibernetinio saugumo subjektas turi vykdyti sutartyje su tiekėju nurodytų kibernetinio saugumo reikalavimų įgyvendinimo kontrolę.** **39. Kibernetinio saugumo subjektas turi būti sudaręs tiekėjų sąrašą, jį tvarkyti ir pasikeitus sutartims peržiūrėti ir atnaujinti numatytu**	

	periodiškumu ir kai įvyksta reikšmingi pokyčiai arba reikšmingi incidentai, susiję su tiekėjais.	
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;	**Kibernetinio saugumo reikalavimų aprašas, tvirtinamas Nutarimo projektu.** **Septintasis skirsnis. Tinklų ir informacinių sistemų įsigijimas, plėtojimas ir priežiūros saugumas, įskaitant spragų valdymą ir atskleidimą** **40. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi nustatyti tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumo užtikrinimo tvarką, kuri apimtų:** **40.1. tinklų ir informacinių sistemų įsigijimo ir diegimo reikalavimus;** **Dešimtasis skirsnis. Kriptografijos ir šifravimo naudojimo politika ir procedūros** **55. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi nustatyti kriptografijos ir šifravimo naudojimo tvarką, apimančią:** **55.1. kibernetinio saugumo subjekto kriptografijos ir šifravimo priemonių naudojimo nuostatas, atsižvelgiant į kibernetinio saugumo subjekto nustatytus informacijos klasifikavimo ir tvarkymo reikalavimus;** **55.2. raktų valdymą (generavimas, sunaikinimas, archyvavimas ir kt.).** **56. Praradus kriptografinį raktą turi būti informuojamas atsakingas asmuo.** **57. Kibernetinio saugumo subjektams taikomi techniniai reikalavimai nurodyti 4 lentelėje.**	Visiškas
21 straipsnis. Kibernetinio saugumo rizikos valdymo priemonės		
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.	**Kibernetinio saugumo reikalavimų aprašas, tvirtinamas Nutarimo projektu.** **Šeštasis skirsnis. Tiekimo grandinės saugumas** **32. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi nustatyti tiekimo grandinės saugumo valdymo tvarką, taikomą paslaugų, darbų ar įrangos pirkimams, susijusiems su tinklų ir informacinių sistemų projektavimu, kūrimu, diegimu, naudojimu, priežiūra, modernizavimu ir (ar) kibernetinio saugumo užtikrinimu, siekiant mažinti galimas kilti rizikas tinklų ir informacinėms sistemoms.**	Visiškas

	33. Kibernetinio saugumo subjektas, nustatydamas tiekimo grandinės saugumo valdymo tvarką, turi numatyti tinklų ir informacinių sistemų tiekėjų atrankos kriterijus, apimančius: **33.1. tiekėjo atitiktį Apraše nustatytiems kibernetinio saugumo reikalavimams;** **33.2. kokybės reikalavimus tinklų ir informacinių sistemų produktams, paslaugoms;** **33.3. prieigų valdymą, įskaitant prieigų laikotarpio ribojimą.** **34. Kibernetinio saugumo subjektas sutartyse su tiekėjais (įskaitant subtiekėjus), kiek tai susiję su teikiamomis paslaugomis, turi numatyti:** **34.1. tiekėjo atitikties šiam Aprašui reikalavimus;** **34.2. tiekėjo personalui reikalingus įgūdžius ir (ar) mokymus, ir (ar) sertifikatus, ir (ar) kvalifikaciją;** **34.3. tiekėjo pareigą pranešti kibernetinio saugumo subjektui apie visus didelius ir (ar) kitus incidentus, susijusius su kibernetinio saugumo subjekto tinklų ir informacinėmis sistemomis, kai tik tiekėjas sužino apie incidentą, ir pateikti kibernetinio saugumo subjektui kibernetinio incidento tyrimo ataskaitą;** **34.4. teisę kibernetinio saugumo subjektui arba jo įgaliotiems paslaugų teikėjams atlikti tiekėjo atitikties Aprašui auditą (įskaitant neplaninį) ir tiekėjo pareigą sudaryti sąlygas tokiam auditui atlikti sutarties vykdymo laikotarpiu ar įvykus dideliam incidentui;** **34.5. pareigą užtikrinti spragų, keliančių riziką kibernetinio saugumo subjekto tinklams ir informacinėms sistemoms, valdymą;** **34.6. konfidencialumo ir duomenų neatskleidimo įsipareigojimus;** **34.7. paslaugų teikimo lygmenis (angl. *Service Level Agreement,* SLA);** **34.8. apibrėžti tiekėjų prieigos (loginės ir fizinės) prie tinklų ir informacinės sistemos lygius ir sąlygas;** **34.9. numatyti reikalavimus, keliamus tiekėjo patalpoms, įrangai, tinklų ir informacinių sistemų priežiūrai, informacijos perdavimui tinklais;** **34.10. numatyti tiekėjo ir kibernetinio saugumo subjekto teises ir pareigas.** **35. Kibernetinio saugumo subjektas, tvirtindamas tiekimo grandinės saugumo valdymo tvarką, turi numatyti tinklų ir informacinių sistemų paslaugų teikėjų rizikos vertinimo reikalavimus.**	
23 straipsnis. Pareigos pranešti		

<table>
<tr>
<td>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.</td>
<td>Nacionalinis kibernetinių incidentų valdymo planas, tvirtinamas Nutarimo projektu.

20. NKSC, Lietuvos policija ir Valstybinė duomenų apsaugos inspekcija, gavę informacijos apie kibernetinius incidentus arba juos nustatę, nedelsdami, bet ne vėliau kaip per 24 valandas nuo informacijos gavimo ar nustatymo momento kibernetinius incidentus registruoja Platformoje teikdami visą turimą informaciją ir apie tai informuoja kibernetinio saugumo subjektų Saugumo operacijų centrą. Apie institucijų užregistruotus kibernetinius incidentus kibernetinio saugumo subjektų Saugumo operacijų centrai informuojami per Platformą. Kibernetinio saugumo subjekto Saugumo operacijų centras Plane nustatytais terminais privalo pateikti Kibernetinio saugumo įstatymo 18 straipsnio 4 dalies 1 arba 2 punkte nurodytą informaciją.

Nacionalinio kibernetinių incidentų valdymo proceso 4 priedas.
Nacionalinio kibernetinių incidentų valdymo proceso aprašymo veiksmai:
<table>
<tr><th>Eil. Nr.</th><th>Veiksmo aprašymas</th><th>Dalyvis</th><th>Terminai</th><th>Rezultatas</th></tr>
<tr><td>7.</td><td>Įvertinti, ar siųsti NKSC.

Įvertinus tikimybę kibernetiniam incidentui tapti ekstremaliuoju įvykiu, priimamas sprendimas pateikti rekomendacijas arba siųsti ekspertus (skirti resursus).</td><td>NKSC</td><td>Nedelsiant, bet ne vėliau kaip per 24 val.</td><td>Priimtas sprendimas teikti rekomendacijas arba siųsti ekspertus (skirti resursus).</td></tr>
</table>
</td>
<td>Visiškas</td>
</tr>
</table>

8.	**Informuoti** **Kibernetinio saugumo subjektas informuojamas apie sprendimą nesiųsti ekspertų. Šiuo atveju pateikiamos kibernetinio incidento valdymo rekomendacijos.**	**NKSC**	**Nedelsiant.**	**Informuotas kibernetinio saugumo subjektas, pateiktos rekomendacijos.**

<...>

10.	**Įvertinti kibernetinio incidento poveikį.** **Vertinamas kibernetinio incidento poveikis ir sprendžiama, ar kibernetinis incidentas atitinka Kibernetinio saugumo įstatyme ir Plane nustatytus didelio kibernetinio incidento kriterijus.**	**NKSC**	**Nuolat.**	**Nustatytas kibernetinio incidento poveikis.**
11.	**Įvertinti, ar yra krizės indikatorių.** **Vertinama, ar kibernetinis incidentas atitinka ypatingo ar ekstremaliojo įvykio kriterijus.**	**NKSC**	**Nuolat, iki bus suvaldytas kibernetinis incidentas.**	**Nustatyta, ar yra kibernetinės krizės indikatorių.**

	12.	**Informuoti.** **Užregistravus kibernetinį incidentą, atitinkantį ekstremaliojo įvykio kriterijus, arba nustačius atitinkamą grėsmę, taip pat galimą arba susidariusią kibernetinę krizę, Vyriausybės nustatyta Pranešimo ir keitimosi informacija apie įvykį, ekstremalųjį įvykį, ypatingą įvykį, ekstremaliąją situaciją ar krizę tvarkos aprašo nustatyta tvarka informuojamas Nacionalinis krizių valdymo centras (toliau – NKVC).**	**NKSC**	**Nedelsiant, bet ne vėliau kaip per 1 valandą.**	**Pateikta informacija NKVC.**	
	13.	**Skirti resursus kibernetiniam incidentui valdyti.** **Nustačius, kad kibernetinis incidentas atitinka ypatingo**	**NKSC**	**Nedelsiant.**	**Priimtas sprendimas dėl resursų skyrimo.**	

		ar ekstremaliojo įvykio kriterijus, šių įvykių grėsmę, taip pat galimą arba susidariusią kibernetinę krizę, sprendžiama dėl resursų, reikalingų kibernetiniam incidentui suvaldyti, skyrimo. **Priėmus sprendimą skirti resursus kibernetiniam incidentui suvaldyti, siunčiami ekspertai, o kibernetinis incidentas toliau valdomas atsižvelgiant į NKSC ekspertų rekomendacijas ir įžvalgas, privalomus nurodymus.**				
	14.	**Nustatyti, ar suvaldytas kibernetinis incidentas** **Vykdant kibernetinio incidento valdymo stebėseną vertinama kibernetinio saugumo subjekto pateikiama informacija ir vertinama, ar yra poreikis teikti rekomendacijas.**	**NKSC**	**Nedelsiant.**	**Įvertinta, ar kibernetinis incidentas suvaldytas.**	

15.	**Pateikti kibernetinio incidento valdymo rekomendacijas.** **Priėmus sprendimą dėl rekomendacijų teikimo būtinumo, teikiami siūlymai pagal geriausias praktikas.**	**NKSC**	**Nedelsiant.**	**Pateiktos rekomendacijos.**
16.	**Pateikti kibernetinių incidentų prevencijos rekomendacijas.** **Rengiamos ir viešai skelbiamos geriausios praktikos ir kibernetinių incidentų prevencijos ir valdymo rekomendacijos.**	**NKSC**	**NKSC direktoriaus nustatytais terminais.**	**Parengtos ir paskelbtos kibernetinių incidentų prevencijos ir valdymo rekomendacijos.**

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.	**KSĮ** **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; <...> 18) bendradarbiauja su Europos Sąjungos valstybių narių, NATO valstybių narių 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. Vykdant tarpinstitucinį bendradarbiavimą tvarkomos informacijos 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. **Nacionalinis kibernetinių incidentų valdymo planas, tvirtinamas Nutarimo projektu.** **22. Kai didelis kibernetinis incidentas yra susijęs su dviem ar daugiau valstybių narių, NKSC apie didelį kibernetinį incidentą ne vėliau kaip per 24 valandas nuo sužinojimo apie jį momento informuoja kitas paveiktas valstybes nares ir Europos Sąjungos tinklų ir informacijos apsaugos agentūrą (toliau – ENISA).**	Visiškas
8. CSIRT arba kompetentingos institucijos prašymu bendrasis kontaktinis punktas perduoda pagal 1 dalį gautus pranešimus kitų paveiktų valstybių narių bendriesiems kontaktiniams punktams.	**KSĮ** **7 straipsnis. Nacionalinis kibernetinio saugumo centras**	

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.	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; <...> 18) bendradarbiauja su Europos Sąjungos valstybių narių, NATO valstybių narių 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; **Nacionalinis kibernetinių incidentų valdymo planas, tvirtinamas Nutarimo projektu.** **23. NKSC kas 3 mėnesius teikia ENISA suvestinę ataskaitą, į kurią įtraukiami nuasmeninti ir suvestiniai duomenys apie kibernetinius incidentus, kibernetines grėsmes ir vos neįvykusius kibernetinius incidentus.**	Visiškas
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	**KSĮ** **20 straipsnis. Tarpinstitucinis bendradarbiavimas** 1. Kibernetinio saugumo politiką formuojančios ir įgyvendinančios institucijos bendradarbiauja tarpusavyje ir su kitomis valstybės institucijomis, įskaitant Ryšių reguliavimo tarnybą, kompetentingas institucijas pagal Reglamentą (ES) Nr. 910/2014 ir 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentą (ES) 2022/2554 dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011, taip pat Nacionaliniu krizių valdymo centru, 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. **Nacionalinis kibernetinių incidentų valdymo planas, tvirtinamas Nutarimo projektu.**	Visiškas

	24. Informaciją apie didelius kibernetinius incidentus, kibernetinius incidentus, kibernetines grėsmes ir vos neįvykusius kibernetinius incidentus, apie kuriuos pranešė kibernetinio saugumo subjektai, kurie Krizių valdymo ir civilinės saugos įstatymo nustatyta tvarka buvo pripažinti ypatingos svarbos subjektais, NKSC praneša NKVC ne vėliau kaip per 24 valandas nuo sužinojimo apie juos momento. Apie užregistruotus didelius kibernetinius incidentus kibernetinio saugumo subjektuose, kurie Krizių valdymo ir civilinės saugos įstatymo nustatyta tvarka buvo pripažinti ypatingos svarbos subjektais, NKSC praneša NKVC nedelsdamas, bet ne vėliau kaip per 1 valandą nuo kibernetinio incidento užregistravimo. Suvestinę informaciją apie kibernetinius incidentus, kibernetines grėsmes ir vos neįvykusius kibernetinius incidentus šiame punkte nurodytuose kibernetinio saugumo subjektuose NKSC pateikia NKVC kas 3 mėnesius	

_____