

## DIREKTYVOS (ES) 2022/2555 IR NACIONALINIŲ TEISĖS AKTŲ ATITIKTIES LENTELĖ

<p><b>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)</b></p>	<p>Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymo Nr. XIV-2902 projektas (toliau – KSĮ projektas)</p>	<p><b>Direktyvos perkėlimo, įgyvendinimo lygis (visiškas, dalinis)</b></p>
<p><b>3 straipsnis. Esminiai ir svarbūs subjektai</b></p> <p>1. Šios direktyvos taikymo tikslais esminiais subjektais laikomi šie subjektai:</p> <p>a) I priede nurodytos rūšies subjektai, kurie viršija vidutinėms įmonėms nustatytas viršutines ribas, nustatytas Rekomendacijos 2003/361/EB priedo 2 straipsnio 1 dalyje;</p> <p>&lt;...&gt;</p> <p>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 identifikojo kaip esminius subjektus pagal 2 straipsnio 2 dalies b–e punktus.</p>	<p><b>KSĮ projektas</b></p> <p><b>11 straipsnis. Kibernetinio saugumo subjektai</b></p> <p>&lt;...&gt;</p> <p>3. Bendrieji esminių subjektų identifikavimo kriterijai:</p> <p>1) subjektas teikia paslaugas ir (ar) vykdo veiklą šio įstatymo 1 priede nurodytuose sektoriuose ir viršija vidutinių įmonių darbuotojų skaičių ir <b>(ar) abi</b> finansinius duomenis apibrėžiančias ribas, nustatytas Smulkiojo ir vidutinio verslo plėtros įstatyme;</p> <p>&lt;...&gt;</p> <p>4. Bendrieji svarbių subjektų identifikavimo kriterijai:</p> <p>1) subjektas teikia paslaugas ir (ar) vykdo veiklą šio įstatymo 2 priede nurodytuose sektoriuose, viršija mažų įmonių darbuotojų skaičių ir <b>(ar) abi</b> finansinius duomenis apibrėžiančias ribas, nustatytas Smulkiojo ir vidutinio verslo plėtros įstatyme, ir šio subjekto šiame punkte nurodytų teikiamų paslaugų ir (ar) vykdomos veiklos metinių pajamų suma viršija 50 procentų visų subjekto metinių pajamų;</p> <p>2) subjektas teikia paslaugas ir (ar) vykdo veiklą šio įstatymo 1 priede nurodytuose sektoriuose ir viršija mažų įmonių darbuotojų skaičių ir <b>(ar) abi</b> finansinius duomenis apibrėžiančias ribas, tačiau neviršija vidutinių įmonių darbuotojų skaičiaus ir <b>bent vienos</b> iš finansinių duomenų ribos, nustatytos Smulkiojo ir vidutinio verslo plėtros įstatyme;</p> <p>&lt;...&gt;</p> <p><b>8. Identifikuojant kibernetinio saugumo subjektus pagal šio straipsnio 3 dalies 1 ir 3 punktuose, 4 dalies 1–4 punktuose nustatytą vidutinių įmonių darbuotojų skaičiaus kriterijų, remiamasi Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos turimais duomenimis apie apdraustuosius asmenis. Jei identifikuojant kibernetinio saugumo subjektus apskaičiuotas subjekto vidutinis darbuotojų skaičius nesutampa su apskaičiuotu Smulkiojo ir vidutinio verslo plėtros įstatymo 3 straipsnio 7 dalyje nustatyta tvarka, remiamasi subjekto pateiktais duomenimis, apskaičiuotais vadovaujantis Smulkiojo ir vidutinio verslo plėtros įstatymo 3 straipsnio 7 dalyje nustatyta tvarka.</b></p>	<p>Visiškas</p>

	<p><b>9. Identifikuojant kibernetinio saugumo subjektus pagal šio straipsnio 3 dalies 1 ir 3 punktuose, 4 dalies 1–4 punktuose nustatytus kriterijus, juridinių asmenų atveju remiamasi duomenimis apie metines pajamas bei įmonės balanse nurodyto turto vertę. Šie duomenys nustatomi pagal Juridinių asmenų registro duomenų tvarkytojui pateiktą įmonės metinių finansinių ataskaitų rinkinį ar įmonių grupės metinių finansinių konsoliduotųjų ataskaitų rinkinį, kai jų teikimas privalomas, arba pagal mokesčių administratoriaus turimus duomenis, kai finansinių ataskaitų rinkinių teikimas neprivalomas. Fizinį asmenų atveju remiamasi mokesčių administratoriaus turimais duomenimis apie fizinio asmens individualios veiklos pajamas, kaip jos suprantamos pagal Lietuvos Respublikos gyventojų pajamų mokesčio įstatymą.</b></p>	
<p>4. Siekdamas sudaryti 3 dalyje nurodytą sąrašą, valstybės narės reikalauja, kad toje dalyje nurodyti subjektai kompetentingoms institucijoms pateiktų bent šią informaciją:</p> <p>&lt;...&gt;</p> <p>b) adresą ir naujausius kontaktinius duomenis, įskaitant subjektų el. pašto adresus, IP adresų ruožus ir telefonų numerius;</p> <p>&lt;...&gt;</p>	<p><b>KSĮ projektas</b></p> <p><b>13 straipsnis. Kibernetinio saugumo subjektų registras</b></p> <p>&lt;...&gt;</p> <p>3. Kibernetinio saugumo subjektų registrą sudaro šie pagrindiniai duomenys apie kibernetinio saugumo subjektus:</p> <p>1) jeigu kibernetinio saugumo subjektas yra juridinis asmuo – kibernetinio saugumo subjekto pavadinimas, juridinio asmens kodas, teisinė forma, ekonominės veiklos <del>sritis</del> <del>(sritis)</del> ir rūšis (rūšys), pagrindinės buveinės adresas, o jeigu kibernetinio saugumo subjektas nėra įsisteigęs Europos Sąjungoje; – pagal šio įstatymo 12 straipsnio 3 dalį paskirto atstovo pavadinimas, teisinė forma, ekonominės veiklos <del>sritis</del> <del>(sritis)</del> ir rūšis (rūšys), adresas. Jeigu kibernetinio saugumo subjektas yra DNS paslaugų teikėjas, aukščiausio lygio domenų vardų registravimo paslaugas teikiantis subjektas, debesijos paslaugų teikėjas, duomenų centrų paslaugų teikėjas, paskirstytojo turinio teikimo tinklo paslaugų teikėjas, valdomų paslaugų teikėjas, valdomų kibernetinio saugumo paslaugų teikėjas, elektroninės prekyvietės paslaugų teikėjas, interneto paieškos sistemų, <del>ir</del> socialinių tinklų paslaugų platformų paslaugų teikėjas <b>ir patikimumo užtikrinimo paslaugų teikėjas</b> (toliau – specialusis subjektas) ar yra domenų vardų registravimo paslaugas teikiantis subjektas – ir kitų juridinių padalinių Europos Sąjungoje adresai;</p> <p>&lt;...&gt;</p>	Visiškas
<p><b>7 straipsnis. Nacionalinė kibernetinio saugumo strategija</b></p> <p>2. Nacionalinėje kibernetinio saugumo strategijoje valstybės narės visų pirma nustato:</p> <p>h) politiką, įskaitant atitinkamas procedūras ir tinkamas dalijimosi informacija priemones, siekiant remti savanorišką dalijimąsi kibernetinio saugumo informacija tarp subjektų laikantis Sąjungos teisės;</p>	<p><b>KSĮ projektas</b></p> <p><b>19 straipsnis. Kibernetinio saugumo informacinė sistema</b></p> <p>&lt;...&gt;</p> <p>4. Kibernetinio saugumo subjektai turi teisę tapti Kibernetinio saugumo informacinės sistemos <del>naudotojais</del> <b>nariais</b>, įgyvendindami tarpusavio dalijimosi kibernetinio saugumo informacija susitarimus. Nepriklausomai nuo to, ar naudojamosi Kibernetinio saugumo informacine sistema, kibernetinio saugumo subjektai privalo pranešti Nacionaliniam</p>	Visiškas

	kibernetinio saugumo centrui apie tokių susitarimų sudarymą, taip pat apie pasitraukimą iš tokių susitarimų per 20 darbo dienų nuo šių aplinkybių atsiradimo dienos.	
<b>10 straipsnis. Reagavimo į kompiuterių saugumo incidentus tarnybos (CSIRT)</b> 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.	<b>KSĮ projektas</b> <b>19 straipsnis. Kibernetinio saugumo informacinė sistema</b> 1. Kibernetinio saugumo informacinės sistemos paskirtis: <...> 5) keistis su <b>subjektais, atitinkančiais Kibernetinio saugumo informacinės sistemos nuostatuose nustatytus reikalavimus ir turinčiais teisę prisijungti prie Kibernetinio saugumo informacinės sistemos naudotojais (toliau – Kibernetinio saugumo informacinės sistemos nariai)</b> , duomenimis, susijusiais su kibernetiniais incidentais, kibernetinėmis grėsmėmis, vos neįvykusiais kibernetiniais incidentais, taip pat kita su kibernetinio saugumo užtikrinimu susijusia informacija; <...>	Visiškas
<b>13 straipsnis. Bendradarbiavimas nacionaliniu lygmeniu</b> 6. Valstybės narės techninėmis priemonėmis supaprastina informacijos, susijusios su 23 ir 30 straipsniuose nurodytais pranešimais, teikimą.	<b>KSĮ projektas</b> <b>19 straipsnis. Kibernetinio saugumo informacinė sistema</b> 1. Kibernetinio saugumo informacinės sistemos paskirtis: <...> 5) keistis su <b>subjektais, atitinkančiais Kibernetinio saugumo informacinės sistemos nuostatuose nustatytus reikalavimus ir turinčiais teisę prisijungti prie Kibernetinio saugumo informacinės sistemos naudotojais (toliau – Kibernetinio saugumo informacinės sistemos nariai)</b> , duomenimis, susijusiais su kibernetiniais incidentais, kibernetinėmis grėsmėmis, vos neįvykusiais kibernetiniais incidentais, taip pat kita su kibernetinio saugumo užtikrinimu susijusia informacija;	Visiškas
<b>26 straipsnis. Jurisdikcija ir teritoriškumas</b> 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.	<b>KSĮ projektas</b> <b>12 straipsnis. Jurisdikcija ir teritoriškumas</b> <...> 2. <del>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 narė, 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 narė, kurioje įgyvendinamos kibernetinio saugumo rizikos valdymo priemonės, laikoma, kad pagrindinė</del>	Visiškas

	buveinė yra Lietuvos Respublikoje, jeigu subjektas Lietuvos Respublikoje turi padalinį, kuriame dirba daugiausia jo darbuotojų Europos Sąjungoje.	
<p><b>27 straipsnis. Subjektų registras</b></p> <p>2. Valstybės narės reikalauja, kad 1 dalyje nurodyti subjektai kompetentingoms institucijoms ne vėliau kaip 2025 m. sausio 17 d. pateiktų šią informaciją:</p> <p>&lt;...&gt;</p> <p>c) subjekto pagrindinės buveinės adresą ir kitus juridinius padalinius Sąjungoje arba, jei jie nėra įsisteigę Sąjungoje, pagal 26 straipsnio 3 dalį paskirto atstovo adresą;</p> <p>&lt;...&gt;</p>	<p><b>KSĮ projektas</b></p> <p><b>13 straipsnis. Kibernetinio saugumo subjektų registras</b></p> <p>&lt;...&gt;</p> <p>3. Kibernetinio saugumo subjektų registrą sudaro šie pagrindiniai duomenys apie kibernetinio saugumo subjektus:</p> <p>1) jeigu kibernetinio saugumo subjektas yra juridinis asmuo – kibernetinio saugumo subjekto pavadinimas, juridinio asmens kodas, teisinė forma, ekonominės veiklos <del>sritis (sritys)</del> ir rūšis (rūšys), pagrindinės buveinės adresas, o jeigu kibernetinio saugumo subjektas nėra įsisteigęs Europos Sąjungoje, – pagal šio įstatymo 12 straipsnio 3 dalį paskirto atstovo pavadinimas, teisinė forma, ekonominės veiklos <del>sritis (sritys)</del> ir rūšis (rūšys), adresas. Jeigu kibernetinio saugumo subjektas yra DNS paslaugų teikėjas, aukščiausio lygio domenų vardų registravimo paslaugas teikiantis subjektas, debesijos paslaugų teikėjas, duomenų centrų paslaugų teikėjas, paskirstytojo turinio teikimo tinklo paslaugų teikėjas, valdomų paslaugų teikėjas, valdomų kibernetinio saugumo paslaugų teikėjas, elektroninės prekyvietės paslaugų teikėjas, interneto paieškos sistemų, <del>ir</del> socialinių tinklų paslaugų platformų paslaugų teikėjas <b>ir patikimumo užtikrinimo paslaugų teikėjas</b> (toliau – specialusis subjektas) ar yra domenų vardų registravimo paslaugas teikiantis subjektas – ir kitų juridinių padalinių Europos Sąjungoje adresai;</p> <p>&lt;...&gt;</p>	Visiškas
<p><b>29 straipsnis. Dalijimosi kibernetinio saugumo informacija susitarimai</b></p> <p>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 keisti svarbia kibernetinio saugumo informacija, įskaitant informaciją, susijusią su kibernetinėmis grėsmėmis, vos neįvykusiais incidentais, pažeidžiamumais, metodais ir procedūromis, užvaldymo rodikliais, priešiška taktika, konkrečių grėsmių ir dalyvių informacija, kibernetinio saugumo įspėjimais ir rekomendacijomis dėl kibernetinio saugumo priemonių konfigūracijos siekiant aptikti kibernetinius išpuolius, kai tokiu dalijimusi informacija:</p>	<p><b>KSĮ projektas</b></p> <p><b>19 straipsnis. Kibernetinio saugumo informacinė sistema</b></p> <p>&lt;...&gt;</p> <p>3. Kibernetinio saugumo informacinės sistemos <del>naudotojai</del> <b>narai</b> yra subjektai, atitinkantys Kibernetinio saugumo informacinės sistemos nuostatuose nurodytus reikalavimus. Šio straipsnio 1 dalies 6 punkte nustatytus nurodymus duodančios institucijos ir juos įgyvendinantys kibernetinio saugumo subjektai privalo naudotis Kibernetinio saugumo informacinės sistemos dalimi, kurioje tvarkomi duomenys apie privalomus nurodymus blokuoti domeno vardą, identifikuojantį interneto svetainę, nepriklausomai nuo kibernetinio saugumo subjektų atitikties Kibernetinio saugumo informacinės sistemos nuostatuose nurodytiems reikalavimams.</p> <p>4. Kibernetinio saugumo subjektai turi teisę tapti Kibernetinio saugumo informacinės sistemos <del>naudotojais</del> <b>nariais</b>, įgyvendindami tarpusavio dalijimosi kibernetinio saugumo informacija susitarimus. Nepriklausomai nuo to, ar naudojama Kibernetinio saugumo informacinė sistema, kibernetinio saugumo subjektai privalo pranešti Nacionaliniam</p>	Visiškas

<p>a) siekiama užkirsti kelią incidentams, juos atskleisti, į juos reaguoti ar po jų atstatyti veiklą, arba sumažinti jų poveikį;</p> <p>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.</p>	<p>kibernetinio saugumo centrui apie tokių susitarimų sudarymą, taip pat apie pasitraukimą iš tokių susitarimų per 20 darbo dienų nuo šių aplinkybių atsiradimo dienos.</p>	
<p><b>31 straipsnis. Bendrieji aspektai, susiję su priežiūra ir vykdymo užtikrinimu</b></p> <p>1. Valstybės narės užtikrina, kad jų kompetentingos institucijos veiksmingai vykdytų priežiūrą ir imtųsi priemonių, būtinų siekiant užtikrinti, kad būtų laikomasi šios direktyvos.</p>	<p><b>KSĮ projektas</b></p> <p><b>28 straipsnis. Vykdyto užtikrinimo priemonės</b></p> <p>&lt;...&gt;</p> <p>6. Šio straipsnio 1 dalyje nurodytos vykdyto užtikrinimo priemonės taikomos Vyriausybės nustatyta vykdyto užtikrinimo priemonių taikymo <b>kibernetinio saugumo subjektams</b> tvarka.</p> <p>&lt;...&gt;</p>	<p>Visiškas</p>
<p><b>34 straipsnis. Bendrosios administracinių baudų skyrimo esminiams ir svarbiems subjektams sąlygos</b></p> <p>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.</p>	<p><b>KSĮ projektas</b></p> <p><b>30 straipsnis. Baudos</b></p> <p>1. Baudas skiria Nacionalinio kibernetinio saugumo centro vadovas ar jo įgaliotas asmuo Vyriausybės nustatyta vykdyto užtikrinimo priemonių taikymo <del>esminiams ir svarbiems kibernetinio saugumo subjektams</del> tvarka.</p> <p>&lt;...&gt;</p>	<p>Visiškas</p>
<p><b>36 straipsnis. Sankcijos</b></p> <p>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.</p>	<p><b>KSĮ projektas</b></p> <p><b>30 straipsnis. Baudos</b></p> <p>1. Baudas skiria Nacionalinio kibernetinio saugumo centro vadovas ar jo įgaliotas asmuo Vyriausybės nustatyta vykdyto užtikrinimo priemonių taikymo <del>esminiams ir svarbiems kibernetinio saugumo subjektams</del> tvarka.</p> <p>&lt;...&gt;</p>	<p>Visiškas</p>