

**LIETUVOS RESPUBLIKOS
VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ VALDYMO
ĮSTATYMO NR. XI-1807 43 STRAIPSNIO PAKEITIMO ĮSTATYMO PROJEKTO
AIŠKINAMASIS RAŠTAS**

1. Įstatymo projekto rengimą paskatinusios priežastys, parengto projekto tikslai ir uždaviniai

Valstybės informacinių išteklių duomenų sauga, kibernetinis saugumas ir esminės informacinių ir ryšių technologijų infrastruktūros bei elektroninės informacijos saugumo užtikrinimas yra viena iš pagrindinių Septynioliktosios Lietuvos Respublikos Vyriausybės programoje, kuriai Lietuvos Respublikos Seimas pritarė 2016 m. gruodžio 13 d. nutarimu Nr. XIII-82 „Dėl Lietuvos Respublikos Vyriausybės programos“, numatytų Vyriausybės 2016–2020 metų veiklos krypčių.

Šiuo metu galiojančiuose Lietuvos Respublikos įstatymuose ir Vyriausybės nutarimuose išsamiai nedetalizuota, kokia informacija, susijusi su valstybės informacinių išteklių tvarkymu, yra vieša, o kokia turėtų būti laikoma konfidencialia. Taip pat neaišku, kokiais atvejais ši informacija turėtų būti pateikiama pareiškėjams.

Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo Nr. XI-1807 43 straipsnio pakeitimo įstatymo projekto (toliau – Įstatymo projektas) rengimo tikslas – užtikrinti valstybės informacinių išteklių apsaugą.

Įstatymo projekto uždaviniai:

1. informacijai apie valstybės informacinių išteklių tvarkymo saugos priemones ir valstybės informacinių išteklių pažeidžiamumą suteikti konfidencialios informacijos statusą;
2. nustatyti tokios informacijos teikimo sąlygą.

2. Įstatymo projekto iniciatoriai (institucija, asmenys ar piliečių įgalioti atstovai) ir rengėjai

Įstatymo projektą parengė Lietuvos Respublikos krašto apsaugos ministerijos Administracijos departamento (direktorius Audrius Baronas, tel. (8 5) 273 5556, el. p. audrius.baronas@kam.lt) Informacijos apsaugos skyrius (vedėjas Darius Valatkevičius, tel. (8 5) 265 7522, el. p. darius.valatkevicius@kam.lt).

3. Kaip šiuo metu yra reguliuojami Įstatymo projekte aptarti teisiniai santykiai

Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 7 punktą nustato, kad valstybės informacinės sistemos, kitų informacinių sistemų, valstybės registro (kadastro) (toliau – Informacinės sistemos) valdytojas privalo turėti saugos dokumentus: Saugos nuostatus; Saugaus elektroninės informacijos tvarkymo taisykles; Informacinės sistemos veiklos tęstinumo valdymo planą; Informacinės sistemos naudotojų administravimo taisykles. Minėto aprašo 35 ir 36 punktuose nustatyta, kad saugos įgaliotinis kasmet organizuoja visų informacinių sistemų rizikos įvertinimą, o jo rezultatai išdėstomi rizikos įvertinimo ataskaitoje.

Informacinės sistemos saugos dokumentuose detalios aprašomi pagrindiniai informacinės sistemos elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimo, veiklos ir naudojimo procesai, procedūros, o rizikos įvertinimo ataskaitoje pateikiama informacija apie informacinių išteklių pažeidžiamumą – atskleidžiami rizikos veiksniai, galintys turėti įtakos elektroninės informacijos saugai, jų galima žala, pasireiškimo tikimybė ir pobūdis, informacinės sistemos pažeidžiamumas, rizikos valdymo būdai, rizikos priimtumo kriterijus.

Lietuvos Respublikos visuomenės informavimo įstatymo 6 straipsnio 3 dalyje nustatyta, kad valstybės ir savivaldybių institucijos bei įstaigos privalo Lietuvos Respublikos teisės gauti

informaciją iš valstybės ir savivaldybių įstaigų įstatymo (toliau – TGIĮ) bei kitų įstatymų nustatyta tvarka teikti viešąją informaciją. Visuomenės informavimo įstatymo 18 straipsnio 1 ir 2 dalyse nustatyta, kad valstybės ir savivaldybių institucijos bei įstaigos, taip pat kitos įstaigos, įmonės ir organizacijos neteikia viešosios informacijos rengėjams ir (ar) skleidėjams, kitiems asmenims informacijos, kuri pagal įstatymus yra valstybės, tarnybos, profesinės, komercinės ar banko paslaptis arba yra privataus pobūdžio informacija; neteikiama ir ta informacija, kurią teikti draudžia kiti įstatymai, nes jos suteikimas pakenktų valstybės saugumo ir gynybos interesams, baudžiamajam asmenų persekiojimui, skatintų pažeisti valstybės teritorijos vientisumą ar viešąją tvarką arba jos nesuteikimas užkirstų kelią teisės pažeidimams ar būtų labai svarbus žmonių sveikatai apsaugoti.

TGIĮ 15 straipsnio 1 dalies 7 punkte nustatyta, kad institucija atsisako pateikti pareiškėjui dokumentus, jeigu pareiškėjas kreipiasi dėl dokumentų, kurių teikimui TGIĮ nuostatos netaikomos šio įstatymo 2 straipsnio 2 dalyje nurodytais atvejais. TGIĮ 2 straipsnio 2 dalies 3 punkte nustatyta, jog šis įstatymas netaikomas dokumentams, kuriuos teikti draudžia įstatymai ar jų pagrindu priimti kiti norminiai teisės aktai, įskaitant dokumentus, kurie nėra prieinami dėl nacionalinio ar visuomenės saugumo, šalies gynybos interesų, statistinių duomenų slaptumo, komercinio konfidencialumo arba kurie sudaro valstybės, tarnybos, banko, komercinės, profesinės paslaptį.

Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 31 straipsnyje nustatyta, kad, kuriant valstybės informacinę sistemą, jos diegimo dokumentai ir kiti projektiniai dokumentai, išskyrus valstybės informacinės sistemos techninį aprašymą (specifikaciją), yra konfidencialūs ir atskleidžiami tik tuo atveju, jeigu Lietuvos Respublikos įstatymai ar kiti teisės aktai reikalauja juose pateiktą informaciją atskleisti. To paties įstatymo 43 straipsnyje reglamentuojama valstybės informacinių išteklių sauga, tačiau nenumatyti informacijos apie valstybės informacinių išteklių tvarkymo saugos priemonės ir valstybės informacinių išteklių pažeidžiamumą teikimo apribojimai.

4. Kokios siūlomos naujos teisinio reguliavimo nuostatos ir kokių teigiamų rezultatų laukiama

Valstybės informacinių išteklių valdymo įstatymo 43 straipsnyje siūloma nustatyti, kad informacija apie valstybės informacinių išteklių tvarkymo saugos priemonės ir valstybės informacinių išteklių pažeidžiamumą yra konfidenciali. Ši informacija galėtų būti teikiama tik tais atvejais, jeigu galimybė teikti šią informaciją numatyta įstatymuose ar jų pagrindu priimtuose kituose norminiuose teisės aktuose. Jei valstybės informacinių išteklių tvarkymo saugos priemonės bus nustatytos teisės aktuose, kurie, vadovaujantis Lietuvos Respublikos teisėkūros pagrindų įstatymu, registruojami ir skelbiami teisės aktų registre, galimybę su jais susipažinti turės visi asmenys.

Informacijai apie valstybės informacinių išteklių tvarkymo saugos priemonės ir valstybės informacinių išteklių pažeidžiamumą suteikus konfidencialios informacijos statusą, bus sudarytos sąlygos šios informacijos apsaugai ir užkirstas kelias neigiamoms pasekmėms. Saugos priemonių pavišinimas gali sudaryti neteisėto prisijungimo prie informacinės sistemos galimybę, sutrikdyti ar pakeisti informacinės sistemos veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti.

Šiuo metu galiojančio Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 13 punkte nustatyta, kad saugos dokumentai institucijoje turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per metus informacinės sistemos valdytojo vadovo nustatyta tvarka. Saugos dokumentai taip pat turi būti persvarstomi (peržiūrimi) po to, kai atliekamas rizikos įvertinimas ar informacinių technologijų saugos atitikties vertinimas arba institucijoje įvyksta esminių organizacinių, sisteminių ar kitokių pokyčių. Todėl informacinės sistemos ar registro valdytojas, peržiūradamas saugos dokumentus, turės įvertinti, kokios saugos dokumentų turinio

nuostatos, vadovaujantis minėtoju nutarimu, yra perteklinės, ir, atsižvelgdamas į Valstybės informacinių išteklių valdymo įstatymo 43 straipsnio pakeitimu reglamentuotus valstybės informacinių išteklių tvarkymo saugos priemonių teikimo apribojimus, eliminuoti neskelbtiną informaciją.

5. Numatomo teisinio reguliavimo poveikio vertinimo rezultatai, galimos neigiamos priimto įstatymo pasekmės ir kokių priemonių reikėtų imtis, kad tokių pasekmių būtų išvengta
Neigiamų teisinio reguliavimo pasekmių nenumatoma.

6. Kokią įtaką priimtas įstatymas turės kriminogeninei situacijai, korupcijai
Priimtas įstatymas neturės įtakos kriminogeninei situacijai ir korupcijai.

7. Kaip įstatymo įgyvendinimas atsilieps verslo sąlygoms ir jo plėtrai
Priimtas įstatymas neturės tiesioginės įtakos verslo sąlygoms ir jo plėtrai.

8. Įstatymo inkorporavimas į teisinę sistemą, kokius teisės aktus būtina priimti, kokius galiojančius teisės aktus reikia pakeisti ar pripažinti netekusiais galios
Priėmus įstatymą, kitų galiojančių įstatymų keisti nereikės.

9. Ar Įstatymo projektas parengtas laikantis Lietuvos Respublikos valstybinės kalbos, Teisėkūros pagrindų įstatymų reikalavimų, o Įstatymo projekto sąvokos ir jas įvardijantys terminai įvertinti Terminų banko įstatymo ir jo įgyvendinamųjų teisės aktų nustatyta tvarka

Įstatymo projektas parengtas laikantis Valstybinės kalbos, Teisėkūros pagrindų įstatymų reikalavimų ir bendrinės kalbos normų.

Įstatymo projekte nustatytas „valstybės informacinių išteklių pažeidžiamumas“ yra kibernetinio saugumo prasme plačiai vartojama bendrojo pobūdžio formuluotė, kuri suprantama kaip tam tikras valstybės informacinių išteklių trūkumas, kuris gali būti panaudotas sukeliant kibernetinį incidentą. Atsižvelgiant į tai, Įstatymo projekte nesiūloma įtvirtinti naujų sąvokų.

10. Ar Įstatymo projektas atitinka Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos nuostatas ir Europos Sąjungos dokumentus

Įstatymo projektas atitinka Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos nuostatas ir Europos Sąjungos dokumentus.

11. Jeigu įstatymui įgyvendinti reikia įgyvendinamųjų teisės aktų, – kas ir kada juos turėtų priimti

Vėlesnis Įstatymo projekto nuostatų įgyvendinimas numatytas siekiant sudaryti sąlygas – esant poreikiui – valstybės informacinius išteklius valdančioms ir informaciją apie juos teikiančioms institucijoms ir įstaigoms iki įstatymo įsigaliojimo pasirengti teikti informaciją su apribojimais (pakeisti vidaus darbo tvarką reglamentuojančius teisės aktus, peržiūrėti informacinių sistemų saugos dokumentus). Atsižvelgiant į tai, kad aiškus poreikis keisti vidaus darbo tvarką reglamentuojančius teisės aktus ar peržiūrėti informacinių sistemų saugos dokumentus nėra nustatytas, nėra siūloma konkrečioms institucijoms parengti ir priimti reikalingus teisės aktus. Kitų įstatymui įgyvendinti reikalingų įgyvendinamųjų teisės aktų priimti nereikės.

12. Įstatymo projektui įgyvendinti reikalingos išlaidos
Įstatymo projektui įgyvendinti valstybės biudžeto lėšų nereikės.

13. Įstatymo projekto rengimo metu gauti specialistų vertinimai ir išvados
Įstatymo projekto rengimo metu specialistų vertinimų ir išvadų negauta.

14. Įstatymo projekto reikšminiai žodžiai

Įstatymo projekto reikšminiai žodžiai: „valstybės informaciniai ištekliai“, „saugos priemonė“.

15. Kiti, iniciatorių nuomone, reikalingi pagrindimai ir paaiškinimai

Nėra.



Raimundas Karoblis
Krašto apsaugos ministras