LIETUVOS RESPUBLIKOS FINANSŲ MINISTRAS

ĮSAKYMAS DĖL APRIBOJUSIŲ SAVO GALIMYBĘ LOŠTI ASMENŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2017 m. balandžio 14 d. Nr. 1K-146
Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 43 straipsnio 2 dalimi, 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“, 7.1 papunkčiu, 11, 19 ir 26 punktais:

1. T v i r t i n u Apribojusių savo galimybę lošti asmenų registro duomenų saugos nuostatus (pridedama).

2. P a v e d u Lošimų priežiūros tarnybos prie Lietuvos Respublikos finansų ministerijos direktoriui:

2.1. per 7 dienas nuo šio įsakymo įsigaliojimo dienos paskirti Apribojusių savo galimybę lošti asmenų registro saugos įgaliotinį ir administratorių;

2.2. per 30 dienų nuo šio įsakymo įsigaliojimo dienos Lietuvos Respublikos finansų ministerijai pateikti:

2.2.1. Apribojusių savo galimybę lošti asmenų registro naudotojų administravimo taisyklių projektą;

2.2.2. Apribojusių savo galimybę lošti asmenų registro saugaus elektroninės informacijos tvarkymo taisyklių projektą;

2.2.3. Apribojusių savo galimybę lošti asmenų registro veiklos tęstinumo valdymo plano projektą.

Finansų ministras Vilius Šapoka

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2017 m. balandžio 12 d. raštu Nr. 17-2033(2)

PATVIRTINTA
Lietuvos Respublikos finansų ministro
2017 m. balandžio 14 d. įsakymu Nr. 1K-146

APRIBOJUSIŲ SAVO GALIMYBĘ LOŠTI ASMENŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Apribojusių savo galimybę lošti asmenų registro duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato žinybinio Apribojusių savo galimybę lošti asmenų registro (toliau – Registras) elektroninės informacijos saugos politiką.

2. Saugos nuostatuose vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos teisės aktuose, nurodytuose Saugos nuostatų 12 punkte.

3. Saugos nuostatais vadovaujasi Registro valdytojas, Registro tvarkytojas, Registro saugos įgaliotinis (toliau – Saugos įgaliotinis), Registro administratorius (toliau – Administratorius) ir Registro naudotojai (toliau – Naudotojai).

4. Saugos nuostatų tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti Registro elektroninę informaciją.

5. Registro elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

5.1. Registro elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

5.2. darbui su Registro elektronine informacija naudojamų administracinių saugos priemonių įgyvendinimas ir kontrolė;

5.3. Registro elektroninei informacijai tvarkyti naudojamų techninių saugos priemonių kontrolė.

6. Registro valdytojas – Lietuvos Respublikos finansų ministerija, buveinės adresas: Lukiškių g. 2, LT-01512 Vilnius.

7. Registro tvarkytojas – Lošimų priežiūros tarnyba prie Lietuvos Respublikos finansų ministerijos (toliau – Priežiūros tarnyba). Priežiūros tarnybos buveinės adresas: Ukmergės g. 222, LT-07157 Vilnius. Registro tvarkytojas yra ir asmens duomenų tvarkytojas.

8. Registro valdytojas:

8.1. tvirtina saugos politikos įgyvendinimo dokumentus (toliau – saugos dokumentai): Registro saugaus elektroninės informacijos tvarkymo taisykles, Registro veiklos tęstinumo valdymo planą, Registro naudotojų administravimo taisykles;

8.2. koordinuoja Registro tvarkytojo darbą, metodiškai jam vadovauja ir atlieka šio darbo priežiūrą;

8.3. užtikrina, kad būtų paskirtas Registro duomenų valdymo įgaliotinis, Saugos įgaliotinis ir Administratorius;

8.4. nagrinėja Registro tvarkytojo pasiūlymus dėl Registro saugos tobulinimo ir priima su tuo susijusius sprendimus;

8.5. atlieka kitus Registro nuostatuose, Saugos nuostatuose ir kituose teisės aktuose, reglamentuojančiuose Registro elektroninės informacijos tvarkymo teisėtumą ir saugos valdymą, nustatytus veiksmus.

9. Registro tvarkytojas:

9.1. užtikrina Registro elektroninės informacijos tvarkymo teisėtumą ir Registre tvarkomos elektroninės informacijos saugumą bei Registro saugos atitiktį Lietuvos Respublikos teisės aktams, reglamentuojantiems elektroninės informacijos tvarkymą;

9.2. skiria Registro duomenų valdymo įgaliotinį, Saugos įgaliotinį ir Administratorių;

9.3. teikia pasiūlymus Registro valdytojui dėl Registro elektroninės informacijos saugos tobulinimo, saugos dokumentų priėmimo, keitimo arba panaikinimo, taip pat rengia saugos dokumentų projektus ir teikia juos Registro valdytojui;

9.4. atlieka Registro duomenų bazės techninę priežiūrą ir užtikrina nepertraukiamą Registro veikimą;

9.5. užtikrina Registro sąveiką su kitomis informacinėmis sistemomis ir registrais;

9.6. įgyvendina organizacines ir technines priemones, kurios leidžia Registro elektroninę informaciją apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

9.7. reikalauja, kad Naudotojai, turintys teisę naudotis Registro elektronine informacija numatytoms funkcijoms atlikti, laikytųsi reikalavimų, nustatytų Saugos nuostatuose ir kituose saugos dokumentuose, ir prižiūri, kaip jų laikomasi;

9.8. teikia pasiūlymus Registro valdytojui dėl Registro techninių ir programinių priemonių, būtinų Registro elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

9.9. atlieka kitas Registro valdytojo pavestas, Saugos nuostatuose ir kituose saugos dokumentuose jam priskirtas funkcijas.

10. Saugos įgaliotinis:

10.1. teikia Registro tvarkytojui pasiūlymus dėl:

10.1.1. saugos dokumentų priėmimo, keitimo ar panaikinimo;

10.1.2. informacinių technologijų saugos atitikties vertinimo;

10.1.3. Administratoriaus paskyrimo ir reikalavimų Administratoriui nustatymo.

10.2. teikia Administratoriui ir Naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su Registro elektroninės informacijos saugumo užtikrinimu;

10.3. konsultuoja Naudotojus Registro elektroninės informacijos saugos klausimais;

10.4. inicijuoja Administratoriaus ir Naudotojų mokymą elektroninės informacijos saugos klausimais, informuoja juos apie elektroninės informacijos saugos problemas;

10.5. organizuoja kasmetinį Registro rizikos vertinimą;

10.6. ne rečiau kaip kartą per dvejus metus organizuoja informacinių technologijų saugos atitikties vertinimą;

10.7. atsako už Registro elektroninės informacijos saugumo užtikrinimą ir saugos dokumentų reikalavimų vykdymą;

10.8. koordinuoja Registro elektroninės informacijos saugos incidentų tyrimą;

10.9. atlieka kitas Registro tvarkytojo pavestas, Saugos nuostatuose ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą, jam priskirtas funkcijas.

11. Administratorius:

11.1. organizuoja Registro techninės ir programinės įrangos administravimą ir priežiūrą, siekdamas užtikrinti kokybišką ir patikimą jos veikimą;

11.2. diegia ir prižiūri programinę įrangą;

11.3. suteikia Naudotojams prieigos teisę naudotis Registro elektronine informacija, reikalinga jiems priskirtoms funkcijoms atlikti;

11.4. registruoja ir informuoja Saugos įgaliotinį apie Registro elektroninės informacijos saugos incidentus, Saugos įgaliotiniui teikia siūlymus dėl incidentų pašalinimo;

11.5. Registro tvarkytojui teikia siūlymus dėl Registro palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir Registro elektroninės informacijos saugumo užtikrinimo;

11.6. užtikrina, kad tvarkant Registrą nebūtų pažeisti Saugos nuostatų reikalavimai;

11.7. atsako už Registro duomenų bazės duomenų atsarginių kopijų darymą ir saugojimą;

11.8. atlieka kitas Saugos įgaliotinio pavestas, Saugos nuostatuose ir kituose saugos dokumentuose jam priskirtas funkcijas.

12. Registro elektroninės informacijos sauga užtikrinama vadovaujantis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu, Lietuvos Respublikos kibernetinio saugumo įstatymu, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Saugos dokumentų turinio gairių aprašu ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašu, patvirtintais 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“, Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“, Bendraisiais reikalavimais organizacinėms ir techninėms asmens duomenų saugumo priemonėms, patvirtintais Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms asmens duomenų saugumo priemonėms patvirtinimo“ (toliau – Bendrieji reikalavimai organizacinėms ir techninėms asmens duomenų saugumo priemonėms), Lietuvos standartais LST ISO/IEC 27001:2013 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“ ir LST ISO/IEC 27002:2014 „Informacijos technologija. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“, Saugos nuostatais ir kitais teisės aktais, reglamentuojančiais elektroninės informacijos tvarkymo teisėtumą ir elektroninės informacijos saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

13. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo 9.1 ir 9.2 papunkčiais, Registro elektroninė informacija pagal svarbą priskiriama vidutinės svarbos informacijos kategorijai.

14. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo 12.3 papunkčiu, Registras priskiriamas trečiai informacinių sistemų kategorijai.

15. Vadovaujantis Bendraisiais reikalavimais organizacinėms ir techninėms asmens duomenų saugumo priemonėms, Registro asmens duomenų tvarkymas automatiniu būdu priskiriamas antrajam saugumo lygiui.

16. Registro saugos priemonės parenkamos įvertinus galimus rizikos veiksnius, galinčius turėti įtakos Registro elektroninės informacijos konfidencialumui, vientisumui ir prieinamumui.

17. Saugos įgaliotinis, atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, kuri skelbiama Vidaus reikalų ministerijos interneto svetainėje, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, ne rečiau kaip kartą per metus organizuoja Registro rizikos įvertinimą. Minėtą rizikos įvertinimą gali atlikti ir pats Saugos įgaliotinis. Prireikus Saugos įgaliotinis gali organizuoti neeilinį rizikos įvertinimą. Registro rizikos veiksniams vertinti taikoma kokybinė rizikos vertinimo metodika.

18. Registro rizikos įvertinimo rezultatai pateikiami rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos Registro elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Šioje ataskaitoje išdėstomos pagrindinės Registro rizikos valdymo priemonės.

19. Pagrindiniai rizikos veiksniai, galintys turėti įtakos Registro elektroninės informacijos saugumui, yra šie:

19.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);

19.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis Registru Registro elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugos pažeidimai, vagystės ir kita);

19.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

20. Saugos užtikrinimo priemonės parenkamos siekiant užtikrinti Registro veiklos tęstinumą patiriant kuo mažiau išlaidų ir užtikrinant Registro darbą taip, kad būtų išsaugotas Registro elektroninės informacijos konfidencialumas, vientisumas ir prieinamumas.

21. Registro tvarkytojas, atsižvelgdamas į Registro rizikos įvertinimo ataskaitą, prireikus tvirtina Saugos įgaliotinio parengtą rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

22. Remdamasis atliktais Registro saugos atitikties vertinimo rezultatais, Registro tvarkytojas parengia ir Registro valdytojui pateikia tvirtinti pastebėtų trūkumų šalinimo planą, kuriame nurodomi atsakingi vykdytojai ir nustatomi numatytų priemonių įgyvendinimo terminai.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

23. Registro tarnybinėse stotyse neturi veikti programinė įranga, nesusijusi su Registro elektroninės informacijos tvarkymu, Naudotojų ir pačios įrangos administravimu.

24. Registro tarnybinėse stotyse privalo būti naudojama programinė įranga, skirta informacinei sistemai nuo kenksmingos programinės įrangos apsaugoti. Ši programinė įranga turi būti atnaujinama automatiniu būdu ne rečiau kaip kas trys dienos.

25. Registro programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims.

26. Metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą:

26.1. prieigos prie Registro elektroninės informacijos teises gali suteikti tik Administratorius. Naudotojams suteikiamos tik jų funkcijoms vykdyti būtinos teisės;

26.2. prieiga prie Registro elektroninės informacijos yra ribojama pagal numatytus kriterijus (IP adresus);

26.3. užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą iš kitų valstybės institucijų, naudojami saugūs ryšio kanalai, kuriais perduodami šifruoti duomenys.

26.4. elektroninė informacija iš kitų registrų gaunama tik pagal duomenų teikimo ir (ar) gavimo sutartyse nustatytas perduodamų duomenų specifikacijas, perdavimo sąlygas ir tvarką.

27. Programinės įrangos, įdiegtos tarnybinėse stotyse ir Registro tvarkytojo kompiuteriuose, naudojimo nuostatos:

27.1. turi būti naudojama tik legali, Registro funkcionalumui užtikrinti būtina programinė įranga;

27.2. programinė įranga turi būti nuolat atnaujinama laikantis gamintojo reikalavimų;

27.3. programinės įrangos diegimą, šalinimą ir konfigūravimą gali atlikti tik Administratorius;

27.4. turi būti įdiegta galimybė fiksuoti ir kaupti informaciją apie asmenų, kurie naudojosi prieiga prie Registro elektroninės informacijos, atliktus veiksmus.

28. Registro duomenų bazė yra kopijuojama ir saugoma taip, kad įvykus nenumatytai situacijai Registro veikla būtų visiškai atkurta per 12 valandų. Prireikus atkurti atsargines Registro duomenų bazės kopijas turi teisę tik Administratorius. Turi būti periodiškai atliekama kopijų tinkamumo ir saugojimo kontrolė.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

29. Reikalavimai Saugos įgaliotiniui nustatyti Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 20 ir 21 punktuose.

30. Administratorius privalo išmanyti pagrindinius saugos politikos principus, darbą su duomenų perdavimo tinklais, mokėti užtikrinti jų saugumą, taip pat administruoti ir prižiūrėti duomenų bazes, turi būti susipažinęs su saugumo politika ir teisės aktais, standartais ir kitais dokumentais, reglamentuojančiais duomenų tvarkymą Registre.

31. Naudotojai privalo turėti darbo kompiuteriu įgūdžių, mokėti tvarkyti Registro elektroninę informaciją Registro nuostatų nustatyta tvarka ir būti susipažinę su Saugos nuostatais ir saugos politiką reglamentuojančiais dokumentais.

32. Naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veiklos požymių, neveikiančias arba netinkamai veikiančias elektroninės informacijos saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti Saugos įgaliotiniui ir (arba) Administratoriui.

33. Saugos įgaliotinis ne rečiau kaip kartą per dvejus metus inicijuoja Naudotojų mokymą elektroninės informacijos saugos klausimais, įvairiais būdais informuoja juos apie elektroninės informacijos saugos problemas.

V SKYRIUS
NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

34. Tvarkyti Registro elektroninę informaciją gali tik įgalioti Naudotojai, kurie yra susipažinę su Saugos nuostatais ir kitais saugos dokumentais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, bei atsakomybe už saugos dokumentų nuostatų pažeidimus ir pasirašytinai sutikę laikytis juose nustatytų reikalavimų. Pakartotinis supažindinimas yra vykdomas pasikeitus minėtiems dokumentams.

35. Naudotojų supažindinimą su Saugos nuostatais ir kitais saugos dokumentais vykdo Saugos įgaliotinis.

36. Saugos įgaliotinis informuoja Naudotojus apie Saugos nuostatų ir kitų saugos dokumentų pakeitimus. Informacija apie minėtų teisės aktų pakeitimus siunčiama elektroniniu būdu.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

37. Saugos įgaliotinis, Administratorius ir Naudotojai, pažeidę saugos dokumentų, kitų teisės aktų, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, nuostatas, atsako teisės aktų, nustatančių atsakomybę už saugos dokumentų nuostatų pažeidimus, nustatyta tvarka.

_____