LIETUVOS RESPUBLIKOS SUSISIEKIMO MINISTRO
Į S A K Y M A S

DĖL REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2013 m. kovo 27 d. Nr. 3-179
Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo (Žin., 2011, Nr. 163-7739) 24 straipsnio 2 dalies 1 punktu, Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų, patvirtintų Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2003, Nr. 2-45; 2007, Nr. 49-1891; 2008, Nr. 85-3393), 6.1, 8, 9 ir 15 punktais ir atsižvelgdamas į Saugos dokumentų turinio gaires, patvirtintas Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070):

1. T v i r t i n u Registrų ir valstybės informacinių sistemų registro duomenų saugos nuostatus (pridedama).

2. P a v e d u Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriui:

2.1. paskirti Registrų ir valstybės informacinių sistemų registro saugos įgaliotinį ir administratorių;

2.2. per du mėnesius nuo šio įsakymo įsigaliojimo dienos parengti ir Lietuvos Respublikos susisiekimo ministerijai pateikti tvirtinti:

2.2.1. Registrų ir valstybės informacinių sistemų registro saugaus elektroninės informacijos tvarkymo taisyklių projektą;

2.2.2. Registrų ir valstybės informacinių sistemų registro veiklos tęstinumo valdymo plano projektą;

2.2.3. Registrų ir valstybės informacinių sistemų registro naudotojų administravimo taisyklių projektą.

SUSISIEKIMO MINISTRAS RIMANTAS SINKEVIČIUS

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2013 m. kovo 15 d. raštu Nr. 1D-2774(52)

PATVIRTINTA
Lietuvos Respublikos susisiekimo ministro
2013 m. kovo 27 d. įsakymu Nr. 3-179

REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Registrų ir valstybės informacinių sistemų registro duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja elektroninės informacijos saugos valdymą, organizacinius ir techninius reikalavimus, reikalavimus personalui, dirbančiam su Registrų ir

valstybės informacinių sistemų registru (toliau – registras), registro duomenų naudotojų supažindinimo su saugos dokumentais principus.

2. Saugos nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo (Žin., 2011, Nr. 163-7739), Registrų ir valstybės informacinių sistemų registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2012 m. spalio 16 d. nutarimu Nr. 1263 (Žin., 2012, Nr. 122-6146), Bendruosiuose elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuose, patvirtintuose Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2003, Nr. 2-45; 2007, Nr. 49-1891), Saugos dokumentų turinio gairėse, patvirtintose Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070), ir kituose teisės aktuose vartojamas sąvokas.

3. Saugos nuostatų tikslas – nustatyti principus ir taisykles, užtikrinančias saugų ir teisėtą registro duomenų tvarkymą.

4. Registro duomenų saugumo tikslas yra užtikrinti registro duomenų vientisumą ir prieinamumą.

5. Registro duomenų saugumo užtikrinimo prioritetinės kryptys:

5.1. teisėtas, saugus ir kokybiškas registro duomenų tvarkymas;

5.2. teisėtas ir saugus registro duomenų naudojimas.

6. Registro valdytojas – Lietuvos Respublikos susisiekimo ministerija, Gedimino pr. 17, LT-01505 Vilnius.

7. Registro tvarkytojas – Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos (toliau – Komitetas), Gedimino pr. 7, LT-01103 Vilnius.

8. Registro valdytojas vykdo šias funkcijas:

8.1. organizuoja registro veiklą ir jai vadovauja;

8.2. skiria arba paveda registro tvarkytojui skirti saugos įgaliotinį, duomenų valdymo įgaliotinį ir administratorių;

8.3. tvirtina registro saugos politiką įgyvendinančius dokumentus (toliau – saugos dokumentai):

8.3.1. Registrų ir valstybės informacinių sistemų registro saugaus elektroninės informacijos tvarkymo taisykles;

8.3.2. Registrų ir valstybės informacinių sistemų registro veiklos tęstinumo valdymo planą;

8.3.3. Registrų ir valstybės informacinių sistemų registro naudotojų administravimo taisykles;

8.4. prižiūri, kaip laikomasi teisės aktų, susijusių su registro tvarkymu ir duomenų saugumu, reikalavimų;

8.5. priima sprendimą dėl registro informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

8.6. kontroliuoja, kad registras būtų tvarkomas vadovaujantis Lietuvos Respublikos įstatymais, Saugos nuostatais ir kitais teisės aktais.

9. Registro tvarkytojas vykdo šias funkcijas:

9.1. registro valdytojo pavedimu skiria saugos įgaliotinį ir paveda jam organizuoti ir kontroliuoti saugos dokumentų reikalavimų įgyvendinimą;

9.2. registro valdytojo pavedimu skiria duomenų valdymo įgaliotinį;

9.3. registro valdytojo pavedimu skiria administratorių ir paveda jam užtikrinti registro serverio ir registro naudotojų kompiuterizuotų darbo vietų saugų funkcionavimą, registro duomenų bazės administravimą saugos dokumentų ir kitų teisės aktų nustatyta tvarka;

9.4. atlieka registro duomenų bazės techninę priežiūrą ir užtikrina nepertraukiamą registro veiklą;

9.5. įgyvendina tinkamas organizacines ir technines priemones, kurios skirtos duomenims apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip

pat nuo bet kokio kito neteisėto tvarkymo;

9.6. užtikrina, kad registro naudotojai, turintys teisę naudotis registro duomenimis numatytoms funkcijoms atlikti, laikytųsi reikalavimų, nustatytų Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose;

9.7. organizuoja techninių, programinių priemonių, kurios skirtos registrui eksploatuoti, prižiūrėti ir plėtoti, įsigijimą, jų įdiegimą ir modernizavimą, registro techninės, programinės įrangos priežiūrą ir tobulinimą;

9.8. pagal kompetenciją atsako už registro duomenų tvarkymo teisėtumą ir duomenų saugumą bei registro saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams ir Saugos nuostatams.

10. Saugos įgaliotinis, įgyvendindamas registro elektroninės informacijos saugą, atlieka šias funkcijas:

10.1. teikia registro valdytojo ar tvarkytojo, jeigu jis paskyrė saugos įgaliotinį, vadovui pasiūlymus dėl:

10.1.1. administratoriaus skyrimo;

10.1.2. saugos dokumentų priėmimo, keitimo ar panaikinimo;

10.1.3. saugos reikalavimų atitikties vertinimo atlikimo;

10.2. koordinuoja elektroninės informacijos saugos incidentų, įvykusių registre, tyrimą;

10.3. teikia administratoriui privalomus vykdyti nurodymus ir pavedimus;

10.4. konsultuoja registro naudotojus saugaus duomenų tvarkymo klausimais;

10.5. inicijuoja registro naudotojų mokymą duomenų saugumo klausimais, informuoja juos apie elektroninės informacijos saugos problemas;

10.6. organizuoja registro rizikos vertinimą;

10.7. atsako už duomenų saugumo politikos įgyvendinimą ir saugos dokumentų reikalavimų vykdymą;

10.8. atlieka kitas saugos dokumentuose nurodytas ir Saugos nuostatuose jam priskirtas funkcijas.

11. Administratorius:

11.1. suteikia registro naudotojams teisę naudotis duomenimis, reikalingais jiems priskirtoms funkcijoms atlikti;

11.2. įvertina, ar registro naudotojai yra pasirengę darbui;

11.3. informuoja saugos įgaliotinį apie elektroninės informacijos saugos incidentus;

11.4. teikia registro tvarkytojui pasiūlymus dėl duomenų saugumo organizavimo;

11.5. atsako už tai, kad tvarkant registrą nebūtų pažeisti Saugos nuostatų reikalavimai;

11.6. organizuoja registro kompiuterinės ir programinės įrangos administravimą ir priežiūrą, kad būtų užtikrintas kokybiškas ir patikimas jos veikimas;

11.7. kontroliuoja ir prižiūri programinės ir kompiuterinės įrangos diegimo procesus;

11.8. kontroliuoja registro duomenų bazės duomenų atsarginių kopijų darymą, tinkamumą ir saugojimą.

12. Administratorius turi teisę patikrinti (peržiūrėti) registro sąranką ir registro būsenos rodiklius.

13. Tvarkant registro duomenis ir užtikrinant jų saugą, vadovaujamasi šiais teisės aktais:

13.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

13.2. Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais;

13.3. Saugos dokumentų turinio gairėmis;

13.4. Registrų ir valstybės informacinių sistemų registro nuostatais;

13.5. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 (Žin., 2004, Nr. 80-2855);

13.6. Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniais saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro

2008 m. spalio 27 d. įsakymu Nr. 1V-384 (Žin., 2008, Nr. 127-4866);

13.7. Lietuvos Respublikos vidaus reikalų ministerijos išleista metodine priemone „Rizikos analizės vadovas“ (toliau – Rizikos analizės vadovas), Lietuvos ir tarptautiniais grupės „Informacijos technologija. Saugumo technika“ standartais, reglamentuojančiais saugų duomenų tvarkymą;

13.8. Saugos nuostatais, saugos dokumentais ir kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugos politiką ir registro duomenų tvarkymo teisėtumą bei duomenų saugumo valdymą.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

14. Registrui duomenis, informaciją, dokumentus ir (arba) jų kopijas teikia įsteigtų registrų ir valstybės informacinių sistemų valdytojai arba jų įgalioti registrų ar valstybės informacinių sistemų tvarkytojai Registrų ir valstybės informacinių sistemų registro nuostatų nustatyta tvarka.

15. Registras pagal jame tvarkomos elektroninės informacijos svarbą, vadovaujantis Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairių, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymu Nr. 1V-247 (Žin., 2007, Nr. 78-3160), 3.2.1 punktu, yra priskiriamas antrajai kategorijai.

16. Registro elektroninės informacijos sauga Saugos nuostatuose suprantama kaip administracinių, techninių ir programinių priemonių, skirtų duomenų konfidencialumui (su registre tvarkoma elektronine informacija susipažinti turi teisę tik tam įgalioti asmenys), vientisumui (duomenys neturi būti atsitiktinai ar neteisėtai pakeisti ar sunaikinti) ir prieinamumui (duomenys gali būti tvarkomi reikiamu metu) užtikrinti, visuma.

17. Pagrindiniai rizikos veiksniai, galintys turėti įtakos registro duomenų saugumui, yra:

17.1. subjektyvūs netyčiniai (registro duomenų tvarkymo klaidos ir apsirikimai, šių duomenų ištrynimas, klaidingas jų teikimas, fiziniai informacijos technologijų sutrikimai, duomenų perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);

17.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis registro duomenimis, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

17.3. atsitiktinės subjektyvios aplinkybės (darbuotojų praradimas, gaisrai, vandens poveikis, elektros instaliacijos gedimas ir kita);

17.4. nenugalima jėga (*force majeure*).

18. Saugos įgaliotinis, atsižvelgdamas į Rizikos analizės vadovą, Lietuvos ir tarptautinius grupės „Informacijos technologija. Saugumo technika“ standartus, kasmet organizuoja registro rizikos vertinimą. Prireikus, saugos įgaliotinis gali organizuoti neeilinį rizikos vertinimą.

19. Saugos įgaliotinis, įvertinęs galinčius turėti įtakos registro duomenų saugumui rizikos veiksnius, išvardytus Saugos nuostatų 17 punkte, rengia rizikos įvertinimo ataskaitą, kurioje išdėsto pagrindines registro rizikos mažinimo priemones.

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

21. Rizikos veiksnių tikimybės ir registro duomenų bazės duomenų konfidencialumo, vientisumo, prieinamumo pažeidimo žalos vertinimo klasifikacija yra:

21.1. labai maža – 1 balas;

21.2. maža – 2 balai;

21.3. vidutinė – 3 balai;

21.4. didelė – 4 balai;

21.5. labai didelė – 5 balai.

22. Parenkamos tokios saugos priemonės, kad būtų užtikrintas registro veiklos tęstinumas, patiriama kuo mažiau išlaidų ir užtikrinamas saugus registro darbas.

23. Saugos įgaliotinis, siekdamas užtikrinti Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose išdėstytų nuostatų įgyvendinimą ir saugumo politikos laikymosi kontrolę, kasmet iki gruodžio 1 d. organizuoja registro informacinių technologijų saugos reikalavimų atitikties vertinimą.

24. Registro informacinių technologijų saugos reikalavimų atitikties vertinimo metu:

24.1. įvertinama, ar reali duomenų saugumo situacija atitinka Saugos nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų reikalavimus;

24.2. inventorizuojama registro techninė ir programinė įranga;

24.3. tikrinamos registro tvarkymo kompiuterizuotos darbo vietos ir registre įdiegtos programos bei jų sąranka (konfigūracija);

24.4. patikrinama registro naudotojams suteiktų teisių tvarkyti registrą ir jų vykdomų funkcijų atitiktis;

24.5. įvertinama, kaip pasirengta užtikrinti registro veiklos tęstinumą elektroninės informacijos saugos incidento atveju.

25. Atlikęs registro informacinių technologijų saugos reikalavimų atitikties vertinimą, saugos įgaliotinis parengia pastebėtų trūkumų šalinimo planą, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato registro tvarkytojas.

26. Registro duomenų saugumo priemonės turi būti parenkamos atsižvelgiant į Saugos nuostatų 17 punkte išvardytus rizikos veiksnius, galinčius turėti įtakos registro duomenų saugumui.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

27. Registro elektroninės informacijos saugos priemonės parenkamos vadovaujantis konfidencialumo, vientisumo ir prieinamumo principais.

28. Prieigą prie registro suteikia, apriboja ir panaikina administratorius.

29. Teisė dirbti su konkrečia elektronine informacija suteikiama konkrečiam registro naudotojui arba registro naudotojų grupei.

30. Prisijungimo prie kompiuterių tinklo laikas ir trukmė nėra ribojami, registras pasiekiamas visą parą.

31. Registro naudotojų prieiga prie registro duomenų leidžiama tik per registravimosi ir slaptažodžių sistemą.

32. Registro naudotojų prieigos valdymas apibrėžtas registro naudotojų administravimo taisyklėse.

33. Kompiuterizuotose darbo vietose ir tarnybinėse stotyse naudojama centralizuotai valdoma antivirusinė programinė įranga, kuri yra reguliariai atnaujinama automatiniu būdu ne rečiau kaip kartą per dieną.

34. Kenksmingosios programinės įrangos aptikimo priemonės veikia nuolat realiu laiku.

35. Registro naudotojų kompiuterinėse darbo vietose draudžiama naudoti programinę įrangą, nesusijusią su tiesiogine Komiteto veikla ir funkcijomis.

36. Registrui administruoti naudojamas operacines sistemas, techninę ir programinę įrangą, kurios reikia registro naudotojo funkcijoms vykdyti, diegia ir prižiūri registro tvarkytojo Lietuvos Respublikos viešųjų pirkimų įstatymo (Žin., 1996, Nr. 84-2000; 2006, Nr. 4-102) nustatyta tvarka atrinktas paslaugų teikėjas (toliau – Paslaugų teikėjas), kontroliuojamas administratoriaus.

37. Paslaugų teikėjo įsipareigojimai dėl registro elektroninės informacijos saugos užtikrinimo ir atsakomybė išdėstyti paslaugų teikimo sutartyje.

38. Nešiojamieji kompiuteriai prie kompiuterių tinklo gali būti prijungiami ir iš registro tvarkymo patalpų išnešami tik saugos įgaliotiniui leidus.

39. Registro duomenys iš susijusių registrų gaunami automatiniu būdu pagal duomenų

teikimo sutartyse nustatytas specifikacijas ir sąlygas.

40. Registro duomenų bazė yra kopijuojama ir saugoma taip, kad įvykus nenumatytai situacijai registro veikla būtų visiškai atkurta per 24 valandas.

IV. REIKALAVIMAI PERSONALUI

41. Saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, Informacinių technologijų saugos atitikties vertinimo metodika, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais.

42. Administratoriumi gali būti skiriamas darbuotojas, išmanantis darbą su kompiuterių tinklais ir mokantis užtikrinti jų saugumą. Administratorius turi būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais.

43. Registro naudotojai privalo turėti darbo kompiuteriu įgūdžių, būti susipažinę su saugos dokumentais.

44. Registro naudotojai, pastebėję, kad yra saugos dokumentų pažeidimų, nusikalstamos veikos požymių, kad neveikia arba netinkamai veikia duomenų saugumo užtikrinimo priemonės, privalo nedelsdami apie tai pranešti administratoriui.

45. Saugos įgaliotinis, įtaręs neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeisiančią registro saugą (jos konfidencialumą, vientisumą ar prieinamumą), apie tai turi pranešti kompetentingoms institucijoms.

46. Saugos įgaliotinis periodiškai inicijuoja registro naudotojų mokymą elektroninės informacijos saugos klausimais, įvairiais būdais (priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės priimtiems naujiems darbuotojams ir panašiai) informuoja juos apie elektroninės informacijos saugos problemas.

47. Įvykus elektroninės informacijos saugos incidentui, saugos įgaliotinio, administratoriaus ir registro naudotojų veiksmus reglamentuoja Registrų ir valstybės informacinių sistemų registro veiklos tęstinumo valdymo planas.

V. REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

48. Tvarkyti registro duomenis gali tik įgalioti registro naudotojai, kurie yra susipažinę su saugos dokumentais ir pasirašytinai sutikę laikytis saugos dokumentuose nustatytų reikalavimų.

49. Administratorių ir registro naudotojus su Saugos nuostatais ir atsakomybe už jų reikalavimų nesilaikymą pasirašytinai supažindina saugos įgaliotinis per 10 darbo dienų nuo registro įteisinimo, o su saugos dokumentais – per 10 darbo dienų nuo šių dokumentų patvirtinimo.

50. Registro naudotojų supažindinimą su saugos dokumentais ir atsakomybe už saugos dokumentuose nustatytų reikalavimų nesilaikymą pasirašytinai organizuoja saugos įgaliotinis. Saugos įgaliotinis informuoja registro naudotojus apie saugos dokumentų priėmimą, pakeitimą ar pripažinimą netekusiais galios.

VI. BAIGIAMOSIOS NUOSTATOS

51. Saugos įgaliotinis organizuoja saugos dokumentų svarstymą ne rečiau kaip kartą per metus. Saugos dokumentai yra svarstomi atlikus rizikos analizę ar informacinių technologijų saugos reikalavimų atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams Komitete.

52. Saugos įgaliotinis, duomenų valdymo įgaliotinis, administratorius ir registro naudotojai, pažeidę šių Saugos nuostatų ir kitų saugų elektroninės informacijos tvarkymą

reglamentuojančių teisės aktų nuostatas, atsako įstatymų nustatyta tvarka.

_____