LIETUVOS RESPUBLIKOS ŠVIETIMO IR MOKSLO MINISTRO
Į S A K Y M A S

DĖL ŠVIETIMO IR MOKSLO MINISTRO 2006 M. BALANDŽIO 28 D. ĮSAKYMO NR. ISAK-814 „DĖL LICENCIJŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO

2009 m. sausio 30 d. Nr. ISAK-186
Vilnius

Vadovaudamasis Lietuvos Respublikos Vyriausybės 2007 m. balandžio 25 d. nutarimo Nr. 410 „Dėl Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimo Nr. 952 „Dėl duomenų saugos valstybės ir savivaldybių informacinėse sistemose“ pakeitimo“ (Žin., 2007, Nr. 49-1891) 2 punktu:

1. P a k e i č i u Licencijų registro duomenų saugos nuostatus, patvirtintus Lietuvos Respublikos švietimo ir mokslo ministro 2006 m. balandžio 28 d. įsakymu Nr. ISAK-814 „Dėl Licencijų registro duomenų saugos nuostatų patvirtinimo“ (Žin., 2006, Nr. 50-1842), ir išdėstau juos nauja redakcija (pridedama).

2. P a v e d u Švietimo informacinių technologijų centrui (direktorius Vaino Brazdeikis) per 3 mėnesius nuo šio įsakymo įsigaliojimo parengti ir pateikti Lietuvos Respublikos švietimo ir mokslo ministrui tvirtinti Licencijų registro saugaus elektroninės informacijos tvarkymo taisykles, Licencijų registro veiklos tęstinumo valdymo planą, Licencijų registro naudotojų administravimo taisykles.

ŠVIETIMO IR MOKSLO MINISTRAS GINTARAS STEPONAVIČIUS

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2009-01-07 raštu Nr. 1D-97(13)

PATVIRTINTA
Lietuvos Respublikos švietimo ir mokslo ministro 2006 m. balandžio 28 d. įsakymu Nr. ISAK-814
(Lietuvos Respublikos švietimo ir mokslo ministro 2009 m. sausio 30 d. įsakymo Nr. ISAK-186 redakcija)

LICENCIJŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Licencijų registro duomenų saugos nuostatų (toliau – Saugos nuostatai) tikslas – nustatyti ir įgyvendinti organizacines, technines ir kitas priemones, suteikiančias galimybę saugiai rinkti, apdoroti, kaupti, saugoti Licencijų registro (toliau – Registras) objektų duomenis, juos teikti švietimo ir mokslo registrams, informacinėms sistemoms, suinteresuotiems juridiniams ir fiziniams asmenims.

2. Saugos nuostatai parengti pagal Bendruosius elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimus, patvirtintus Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891), Saugos dokumentų turinio gaires, patvirtintas Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070).

3. Saugos nuostatai privalomi Registro tvarkymo įstaigoms.

4. Registro saugos politiką (toliau – saugos politika) apibrėžia Saugos nuostatai, o šią saugos politiką įgyvendina Licencijų registro saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Tvarkymo taisyklės), Licencijų registro veiklos tęstinumo valdymo planas (toliau – Valdymo planas), Licencijų registro naudotojų administravimo taisyklės (toliau – Administravimo taisyklės), kiti teisės aktai, reglamentuojantys Registro duomenų tvarkymo teisėtumą ir saugos valdymą.

5. Saugos politika vykdoma šiomis prioritetinėmis kryptimis:

5.1. įgyvendinant atliekamų veiksmų su Registro duomenimis automatinį stebėjimą ir įrašų kaupimą;

5.2. įgyvendinant prieigos teisių prie Registro duomenų suteikimą ir duomenų vartotojo tapatumo identifikavimą;

5.3. įgyvendinant Registro duomenų kopijavimą, archyve esančių duomenų saugą;

5.4. įgyvendinant Registro duomenų saugą nuo žalingos programinės įrangos poveikio;

5.5. įrengiant saugias Registro tvarkymui skirtas patalpas ir kompiuterizuotas darbo vietas jose;

5.6. įgyvendinant Registro naudotojų kvalifikacijos tobulinimo sistemą;

5.7. įgyvendinant Registro duomenų integralumą su švietimo ir mokslo registrais ir informacinėmis sistemomis;

5.8. įgyvendinant Registro duomenų saugos priemones nuo nesankcionuoto poveikio Registro programinei, techninei įrangai ir (ar) Registro programinės įrangos modifikavimo.

6. Vadovaujančioji registro tvarkymo įstaiga yra Lietuvos Respublikos švietimo ir mokslo ministerija (toliau – Ministerija), buveinės adresas – A. Volano g. 2/7, LT-01516 Vilnius. Vadovaujančioji registro tvarkymo įstaiga yra ir Registro duomenų valdytoja.

7. Registro tvarkymo įstaigos yra Ministerija ir Švietimo informacinių technologijų centras, buveinės adresas – Suvalkų g. 1, LT-03113 Vilnius.

8. Ministerija paveda Švietimo informacinių technologijų centrui skirti saugos įgaliotinį, tvirtina Saugos nuostatus, Tvarkymo taisykles, Valdymo planą, Administravimo taisykles. Ministerija prižiūri Registro saugos politiką reglamentuojančių teisės aktų parengimą ir

įgyvendinimą. Ministerija kompiuterinį duomenų tvarkymą paveda vykdyti Švietimo informacinių technologijų centrui.

9. Švietimo informacinių technologijų centro direktorius turi:

9.1. skirti saugos įgaliotinį ir jam pavesti organizuoti ir kontroliuoti saugos politiką reglamentuojančių teisės aktų įgyvendinimą;

9.2. paskirti Registro administratorių, jam pavesti užtikrinti Registro tarnybinės stoties saugų funkcionavimą, administruoti Registro duomenų bazę Saugos nuostatų ir kitų saugos politiką reglamentuojančių teisės aktų nustatyta tvarka.

10. Saugos įgaliotinis:

10.1. organizuoja ir kontroliuoja šių Saugos nuostatų įgyvendinimą;

10.2. teikia Švietimo informacinių technologijų direktoriui siūlymus dėl saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo ir dėl Registro saugos reikalavimų atitikties vertinimo atlikimo;

10.3. koordinuoja elektroninės informacijos saugos incidentų tyrimą;

10.4. atlieka kitas Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas, susijusias su Registro sauga.

11. Administratorius atlieka funkcijas, susijusias su naudotojų pasirengimo dirbti su Registro įvertinimu, jų teisėmis, Registrą sudarančiais komponentais (kompiuteriais, operacinėmis sistemomis, taikomųjų programų sistemomis, užkardomis, įsilaužimo aptikimo sistemomis, duomenų perdavimo tinklais), Registro pažeidžiamų vietų nustatymu, atitikties saugumo reikalavimams nustatymu.

12. Švietimo informacinių technologijų centro direktoriaus paskirti Registro naudotojai privalo užtikrinti Registro duomenų saugą saugos politiką reglamentuojančių teisės aktų nustatyta tvarka.

13. Registro duomenų sauga užtikrinama vadovaujantis Lietuvos Respublikos valstybės registrų įstatymu (Žin., 1996, Nr. 86-2043; 2004, Nr. 124-4488), Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, Saugos dokumentų turinio gairėmis, Lietuvos standartu LST ISO/IEC 17799:2006, Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais, Saugos nuostatais, Tvarkymo taisyklėmis, Valdymo planu, Administravimo taisyklėmis, kitais teisės aktais, reglamentuojančiais Registro saugų duomenų tvarkymą.

II. REGISTRO ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

14. Registras priskiriamas trečiajai informacinės sistemos kategorijai. Kategorija suteikta vadovaujantis Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymu Nr. 1V-247 (Žin., 2007, Nr. 78-3160; 2008, Nr. 127-4866). Registro duomenis sudaro bendrieji (nurodyti Licencijų registro nuostatuose, patvirtintuose Lietuvos Respublikos švietimo ir mokslo ministro 2005 m. sausio 24 d. įsakymu Nr. ISAK-100 (Žin., 2005, Nr. 12-403) ir technologiniai (Švietimo informacinių technologijų centro tvarkomi) duomenys.

15. Saugos įgaliotinis turi per kalendorinius metus įvertinti rizikos veiksnių tikėtumą Registro duomenims, techninei, programinei įrangai, registravimo dokumentams, patalpoms Švietimo informacinių technologijų centre, išnagrinėti įrašus rizikos veiksnių tikėtumo registravimo žurnale, parengti pirmo pusmečio – iki liepos mėnesio 10 dienos, antro pusmečio – iki kitų metų sausio mėnesio 10 dienos Rizikos ataskaitą, atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos duomenų saugai.

16. Svarbiausi rizikos veiksniai Registro duomenims, programinei, techninei įrangai yra:

16.1. subjektyvūs netyčiniai (duomenų tvarkymo klaidos ir apsirikimai, klaidingų duomenų teikimas, duomenų perdavimo tinklais sutrikimai, programinės įrangos klaidos ir kita);

16.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema duomenims gauti, duomenų pakeitimas, sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, vagystės ir kita) veiksniai;

16.3. nenugalima jėga *(force majeure).*

17. Rizikos įvertinimo ataskaitą tvirtina Švietimo informacinių technologijų centro vadovas.

18. Patvirtintos Rizikos įvertinimo ataskaitos kopiją saugos įgaliotinis paštu siunčia Registro duomenų valdytojui.

19. Registro duomenų valdytojas, atsižvelgdamas į Registro rizikos įvertinimo ataskaitos rezultatus, gali nurodyti Švietimo informacinių technologijų centrui parengti Registro rizikos valdymo priemonių planą, kuriame nurodomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

20. Rizikos veiksnių Registro duomenims, techninei, programinei įrangai, registravimo dokumentams, patalpoms Švietimo informacinių technologijų centre tikėtumui vertinti turi būti naudojama penkiabalė rizikos veiksnių tikėtumo ir žalos vertinimo metodika:

20.1. nereikšmingas rizikos veiksnių tikėtumas, žala – 1 balas;

20.2. mažas rizikos veiksnių tikėtumas, žala – 2 balai;

20.3. vidutinis rizikos veiksnių tikėtumas, žala – 3 balai;

20.4. didelis rizikos veiksnių tikėtumas, žala – 4 balai;

20.5. labai didelis rizikos veiksnių tikėtumas, žala – 5 balai.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

21. Registro naudotojų darbo vietose draudžiama naudoti programinę ir techninę įrangą, nesusijusią su tiesiogine veikla ir funkcijomis, taip pat draudžiamas rinkmenų apsikeitimo programų naudojimas.

Registro naudotojams draudžiama naudoti nešiojamuosius kompiuterius Registro duomenų perdavimui kompiuterių tinklais ne savo darbo vietoje.

22. Registro naudotojų darbo su Registro dokumentais ir duomenimis tvarka nurodyta Licencijų registro nuostatuose.

23. Registro duomenims apsaugoti nuo kenksmingos programinės įrangos Registro tvarkymo įstaigose turi būti naudojamos programinės priemonės (viena iš jų) – S*ymantec Norton Antivirus, McAfee, Virus scan, Panda AntiVirus, Kaspersky AntiVirus* ir atnaujinamos ne rečiau kaip kartą per mėnesį.

24. Prieigai prie Registro duomenų bazės suteikiami Registro naudotojų ir Registro administratoriaus registracijos vardai ir slaptažodžiai.

25. Registro veiklos tęstinumo ir funkcionalumo užtikrinimui duomenys yra periodiškai kopijuojami kas 12 valandų ir saugomi taip, kad avarijos atveju veiklą iš atsarginių kopijų galima būtų atstatyti per 24 valandas. Elektroninių bylų mėnesinės kopijos papildomai turi būti laikomos atskiroje patalpoje ir saugomos užrakintoje nedegioje spintoje.

26. Visuose Registrą tvarkančiuose kompiuteriuose bei serveriuose privalo būti įdiegta antivirusinė sistema ir apsauga nuo nepageidaujamos programinės įrangos.

27. Konkrečios Registro duomenų tvarkymo ir saugumo procedūros išdėstomos Tvarkymo taisyklėse:

27.1. Registre esančios informacijos kategorijų sąrašas ir kiekvienai kategorijai priskirtini duomenys;

27.2. techninių ir kitų saugos priemonių aprašymas, apimantis kompiuterinės įrangos, sisteminės ir taikomosios programinės įrangos, duomenų perdavimo tinklais saugumo užtikrinimo, patalpų ir aplinkos (įėjimo kontrolė, elektros tiekimas, aplinkos drėgnumas,

darbo vietos temperatūra), priešgaisrinė sauga, darbo apskaitos ir kitas priemones informacijos saugai užtikrinti;

27.3. Registro saugą užtikrinantys reikalavimai, keliami nuomojamų ar perkamų Registro funkcionavimui reikalingoms paslaugoms (patalpos, įrangos ir sistemų priežiūra, duomenų perdavimas tinklais ir kitos paslaugos);

27.4. Registro duomenų vientisumo pažeidimų fiksavimo ir pažeistų duomenų atkūrimo tvarka (naudotojų veiksmų registravimas, atsarginės duomenų kopijos, jų saugojimas, saugojimo kontrolė ir kita);

27.5. saugaus duomenų perkėlimo ar perdavimo tvarka, Nuostatų įgyvendinimo kontrolės tvarka;

27.6. duomenų perdavimo tinklais reikalavimai.

28. Siekiant užtikrinti Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose išdėstytų nuostatų įgyvendinimo kontrolę, saugos įgaliotinis kasmet organizuoja informacinių technologijų saugos reikalavimų atitikties vertinimą Registro naudotojų darbo vietose, kurio metu:

28.1. įvertinama Saugos nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų atitiktis realiai duomenų saugos situacijai;

28.2. inventorizuojama Registro techninė ir programinė įranga;

28.3. tikrinamos ne mažiau kaip dešimtyje procentų Registro naudotojų kompiuterinių darbo vietų visuose paslaugų kompiuteriuose įdiegtos programos ir jų konfigūracija, ne vėliau kaip prieš 5 darbo dienas raštu apie tai informavus Registro naudotoją;

28.4. peržiūrima Registro naudotojams suteiktų teisių atitiktis vykdomoms funkcijoms;

28.5. įvertinamas pasiruošimas Registro veiklai atstatyti nenumatytose situacijose;

28.6. atliekama rizikos analizė ir atitinkamai koreguojama Rizikos ataskaita.

29. Atlikęs Registro informacinių technologijų saugos reikalavimų atitikties vertinimą saugos įgaliotinis rengia pastebėtų trūkumų šalinimo planą, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato Ministerija.

30. Registro duomenų kopijų darymo periodiškumas, kopijų saugojimo priemonės, būdai ir vieta, kopijų atkūrimo tvarka, naikinimo tvarka išdėstomi Tvarkymo taisyklėse.

IV. REIKALAVIMAI PERSONALUI

31. Registro objektų duomenis saugiai rinkti, apdoroti, sisteminti, kaupti, saugoti ir teikti gali asmenys, susipažinę su Licencijų registro nuostatais, Registro saugos politiką reglamentuojančiais teisės aktais.

32. Saugos įgaliotinis privalo išmanyti pagrindinius informacijos saugos principus, turėti atitinkamą kvalifikaciją (kvalifikacijos tobulinimo kursai, pradinis saugaus darbo su duomenimis mokymas, ECDL vartotojo sertifikatas ar pan.), darbo su duomenų bazėmis, operacinėmis sistemomis, taikomosiomis programomis patirties.

33. Saugos įgaliotinis turi:

33.1. sugebėti vertinti rizikos veiksnių tikėtumus ir žalos galimybes, organizuoti ir kontroliuoti trūkumų pašalinimą;

33.2. sugebėti vertinti saugos politiką reglamentuojančių teisės aktų įgyvendinimą.

34. Registro administratorius turi:

34.1. išmanyti darbą su kompiuteriniais tinklais;

34.2. turėti Registrui tvarkyti naudojamų sisteminių programinių priemonių *Windows, Unix, Informix,Oracle* administravimo patirties;

34.3. mokėti administruoti ir prižiūrėti registrų ir informacinių sistemų duomenų bazes;

34.4. užtikrinti Registro saugą saugos politiką reglamentuojančių teisės aktų nustatyta tvarka.

35. Registro naudotojai turi:

35.1. turėti pagrindinius darbo su kompiuteriu įgūdžius;

35.2. mokėti tvarkyti Registro duomenis Registro nuostatuose nustatyta tvarka;

35.3. būti supažindinti su duomenų tvarkymą įgyvendinančiais teisės aktais.

36. Registro naudotojams turi būti nuolat rengiami duomenų saugos mokymai, įvairiais būdais primenama apie saugumo problematiką (pvz., priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės naujai priimtiems darbuotojams ir pan.).

37. Duomenų saugos mokymus ir priminimus apie saugumo problematiką vykdo saugos įgaliotinis, taip pat Registro administratorius.

V. REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

38. Registro naudotojai tvarkyti Registro duomenis gali tik susipažinę su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, ir raštu sutikę laikytis jų reikalavimų (pasirašę konfidencialumo sutartį).

39. Registro naudotojai, prieš suteikiant jiems prieigą prie informacijos, turi išklausyti įvadinį mokymą, skirtą supažindinti su saugos politika, saugumo reikalavimais ir teisine atsakomybe.

40. Registro naudotojų supažindinimą su Saugos nuostatais ir kitais saugos politiką įgyvendinančiais teisės aktais bei atsakomybę už šių reikalavimų nesilaikymą pasirašytinai organizuoja saugos įgaliotinis.

VI. BAIGIAMOSIOS NUOSTATOS

41. Saugos nuostatai ir kiti saugos politiką reglamentuojantys teisės aktai iš esmės peržiūrimi ir prireikus keičiami ne rečiau kaip kartą per metus.

42. Registro tvarkymo įstaigos privalo įgyvendinti šiuose Saugos nuostatuose ir kituose teisės aktuose, reglamentuojančiuose Registro duomenų saugų tvarkymą, nustatytas organizacines, technines ir kitas priemones.

43. Saugos įgaliotinis, Registro naudotojai, Registro administratorius raštu įsipareigoja nepažeisti šių Saugos nuostatų ir kitų teisės aktų, reglamentuojančių Registro duomenų saugų tvarkymą.

44. Duomenys apie Registro naudotojų, Registro administratoriaus atliktus veiksmus su Registro duomenimis saugomi neterminuotai.

45. Saugos įgaliotinis, Registro naudotojas, Registro administratorius, pažeidę šių Saugos nuostatų, kitų teisės aktų, reglamentuojančių Registro duomenų saugų tvarkymą, reikalavimus, atsako įstatymų ir kitų teisės aktų nustatyta tvarka.

_____