PATVIRTINTA
Lietuvos Respublikos aplinkos ministro
2011 m. d.
įsakymu Nr.

ŠILTNAMIO EFEKTĄ SUKELIANČIŲ DUJŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Šiltnamio efektą sukeliančių dujų registro (toliau – Registras) duomenų saugos nuostatų (toliau – Nuostatai) tikslas – sudaryti sąlygas saugiai automatizuotu būdu rinkti, apdoroti, kaupti, tvarkyti Registro objektų duomenis, užtikrinant duomenų konfidencialumą, vientisumą ir prieinamumą.

2. Nuostatai reglamentuoja elektroninės informacijos saugos valdymą, organizacinius ir techninius reikalavimus, Registro naudotojų supažindinimo su saugos dokumentais principus.

3. Nuostatai parengti vadovaujantis Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, patvirtintais Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891) (toliau – Bendrieji reikalavimai), 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), 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) (toliau – Techniniai saugos reikalavimai), Saugos dokumentų turinio gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. IV-172 (Žin., 2007, Nr. 53-2070) (toliau – Gairės), Lietuvos Respublikos klimato kaitos valdymo finansinių instrumentų įstatymu (Žin., 2009, Nr. 87-3662), Šiltnamio efektą sukeliančių dujų registro nuostatais, patvirtintais Lietuvos Respublikos Vyriausybės 2010 m. liepos 14 d. nutarimu Nr. 1072 (Žin., 2010, Nr. 88-4657).

4. Nuostatuose vartojamos sąvokos:

Naudotojas – Lietuvos aplinkos apsaugos investicijų fondo (toliau – Fondas) ar Lietuvos Respublikos aplinkos ministerijos (toliau – Ministerija) valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį (toliau – Darbuotojas), turintis teisę naudotis Registro ištekliais numatytoms funkcijoms atlikti.

Saugos įgaliotinis – Fondo paskirtas Darbuotojas, įgyvendinantis elektroninės informacijos saugą informacinėje sistemoje.

Registro administratorius – Fondo paskirtas Darbuotojas atsakingas už Registro naudotojų registravimą, prieigos prie Registro suteikimą ir panaikinimą ir atliekantis kitas jam priskirtas funkcijas.

Registro informacinės sistemos administratorius (toliau – IS administratorius) – Ministerijos paskirtas Darbuotojas, atliekantis Registro techninės ir programinės įrangos priežiūrą.

Kitos Nuostatuose vartojamos sąvokos apibrėžtos Bendruosiuose reikalavimuose, Gairėse ir kituose Lietuvos Respublikos teisės aktuose.

5. Registro saugos politiką, kurią nustato šie Nuostatai, įgyvendinantys dokumentai yra Registro saugaus elektroninės informacijos tvarkymo taisyklės, Registro veiklos tęstinumo valdymo planas ir Registro naudotojų administravimo taisyklės (toliau – saugos politiką įgyvendinantys dokumentai).

6. Registro elektroninės informacijos saugumo tikslas – sudaryti sąlygas saugiai tvarkyti elektroninę informaciją Registre, užtikrinti saugomos ir apdorojamos informacijos vientisumą ir teisingumą.

7. Įgyvendinti šiuos reikalavimus ypač svarbu norint užtikrinti Registro funkcionavimo tęstinumą, saugomos informacijos tikslumą ir Registro duomenų saugą.

8. Elektroninės informacijos saugumą užtikrina Registro techninė ir programinė įranga, Registro tvarkymo įstaiga, Registro naudotojai, Saugos įgaliotinis ir administratoriai.

9. Už informacijos tvarkymo teisėtumą ir informacijos saugą atsako vadovaujančioji Registro tvarkymo įstaiga – Ministerija. Jos buveinė: Jakšto g. 4/9, LT-01105, Vilnius. Ministerija yra ir Registro duomenų valdytoja.

10. Už duomenų tikslumą ir saugą atsako Registro tvarkymo įstaiga – Fondas. Fondo buveinė: Laisvės pr. 3, LT-04215, Vilnius.

11. Registro elektroninės informacijos svarba ir esama saugos padėtis yra nustatoma periodinės rizikos vertinimo metu ir pateikiama Rizikos įvertinimo ataskaitoje.

12. Pagrindinės Registro elektroninės informacijos saugumo užtikrinimo kryptys:

12.1. fizinė elektroninės informacijos apdorojimo priemonių (tarnybinių patalpų, elektroninės informacijos perdavimo įrangos, programinės įrangos) apsauga;

12.2. organizacinių saugaus darbo su Registro elektronine informacija priemonių įgyvendinimas ir kontrolė;

12.3. veiklos tęstinumas.

13. Vadovaujančioji Registro tvarkymo įstaiga:

13.1. užtikrina, kad Registro duomenys būtų tvarkomi vadovaujantis Lietuvos Respublikos įstatymais, Nuostatais ir kitais teisės aktais;

13.2. prižiūri, kaip laikomasi Registro duomenų saugos reikalavimų;

13.3. tvirtina teisės aktus, nustatančius saugų Registro duomenų tvarkymą;

13.4. nagrinėja ir apibendrina Registro tvarkymo įstaigos pasiūlymus dėl Registro veiklos tobulinimo;

13.5. užtikrina, kad Registras veiktų nepertraukiamai, organizuoja Registro techninę priežiūrą;

13.6. atlieka kitas funkcijas, nurodytas Nuostatuose.

14. Registro tvarkymo įstaiga:

14.1. tvarko Registro duomenis;

14.2. užtikrina sąveiką su susijusiais registrais;

14.3. teikia registro duomenis registro duomenų gavėjams;

14.4. užtikrina tinkamą Registro veikimą, Registro duomenų ir dokumentų saugą;

14.5. skiria Saugos įgaliotinį;

14.6. atlieka kitas Nuostatuose nurodytas funkcijas.

15. Saugos įgaliotinis, įgyvendindamas elektroninės informacijos saugą informacinėje sistemoje, atlieka šias funkcijas:

15.1. teikia vadovaujančiajai Registro tvarkymo įstaigai pasiūlymus dėl administratorių paskyrimo;

15.2. teikia vadovaujančiajai Registro tvarkymo įstaigai pasiūlymus dėl saugos dokumentų priėmimo, keitimo ar panaikinimo, Registro saugos reikalavimų atitikties vertinimo atlikimo;

15.3. koordinuoja saugos incidentų, įvykusių Registro sistemose, tyrimą;

15.4. teikia administratoriams privalomus vykdyti nurodymus ir pavedimus;

15.5. periodiškai inicijuoja Registro Naudotojų mokymą informacijos saugos klausimais, įvairiais būdais informuoti juos apie informacijos saugos problematiką;

15.6. atlieka kitas Nuostatuose ir kituose teisės aktuose pavestas funkcijas.

16. Administratoriai atlieka funkcijas, susijusias su Registro Naudotojų pasirengimo dirbti su jomis įvertinimu, Naudotojų teisėmis, Registro sistemą sudarančiais komponentais (kompiuteriais, tarnybinėmis stotimis, operacinėmis sistemomis, duomenų bazių valdymo sistemomis, taikomųjų

programų sistemomis, ugniasienėmis, įsilaužimų aptikimo sistemomis, duomenų perdavimo tinklais), šių komponentų sąranka, pažeidžiamų vietų nustatymu, saugumo reikalavimų atitiktimi.

17. Teisės aktai, kuriais vadovaujamasi tvarkant Registrą ir jo duomenis, užtikrinant jų saugą:

17.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (Žin., 1996, Nr. 63-1479; 2008, Nr. 22-804);

17.2. Bendrieji reikalavimai;

17.3. Lietuvos standartai LST ISO/IEC 27002:2009, LST ISO/IEC 27001:2006, taip pat kiti Lietuvos ir tarptautiniai grupės „Informacijos technologija. Saugumo metodai“ standartai, apibūdinantys saugų duomenų tvarkymą;

17.4. kiti teisės aktai, reglamentuojantys registrų, informacinių sistemų duomenų tvarkymo teisėtumą, naudotojų veiklą ir elektroninių duomenų saugos valdymą.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

18. Remiantis Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairėmis, Registras priskiriamas trečiajai informacinių sistemų kategorijai. Registro duomenų konfidencialumo, vientisumo ir prieinamumo praradimas gali turėti neigiamą įtaką Ministerijos ir Fondo veiklai.

19. Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“ ir Lietuvos standartą LST ISO/IEC 27005:2008, ne rečiau kaip kartą per metus organizuoja rizikos vertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį rizikos įvertinimą. Rizikos veiksnių vertinimas atliekamas kokybiniu rizikos vertinimo metodu.

20. Registro rizikos vertinimas išdėstomas Rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausi rizikos veiksniai yra šie:

20.1. subjektyvūs netyčiniai (duomenų tvarkymo klaidos ir apsirikimai, duomenų ištrynimas, klaidingas duomenų teikimas, duomenų perdavimo tinklų veiklos trikdymai, programinės įrangos klaidos ir kt.);

20.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis sistemomis, duomenų pakeitimas ir sunaikinimas, duomenų perdavimo tinklų veiklos trikdymai, fizinio saugumo pažeidimai ir kt.);

20.3. nenugalima jėga (force majeure) (darbuotojų praradimas, audros, gaisrai, vandens poveikis, elektros instaliacijos gedimai ir kt.).

21. Atsižvelgdama į rizikos įvertinimo ataskaitą, vadovaujančioji Registro tvarkymo įstaiga prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą. Jame be kito ko numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

22. Siekdamas užtikrinti Nuostatų ir saugos politiką įgyvendinančių dokumentų nustatytų reikalavimų įgyvendinimo organizavimą ir kontrolę, Saugos įgaliotinis ne rečiau kaip kartą per dvejus metus organizuoja informacinių technologijų saugos atitikties vertinimą. Jo metu įvertinama realios duomenų saugos situacijos atitiktis Nuostatų reikalavimams

23. Atlikus atitikties vertinimą, rengiamas pastebėtų trūkumų šalinimo planas. Jį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato vadovaujančiosios Registro tvarkymo įstaigos vadovas..

24. Techninės, programinės ir organizacinės elektroninės informacijos saugos priemonės pasirenkamos siekiant užtikrinti saugų Registro darbą ir Registro veiklos tęstinumą, patiriant kuo mažiau išlaidų.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

25. Prieiga prie Registro suteikiama tik autorizuotiems Naudotojams.

26. Kiekvienas Registro Naudotojas yra unikaliai identifikuojamas – Naudotojas savo tapatybę patvirtina naudotojo vardu ir slaptažodžiu.

27. Prieiga Naudotojams suteikiama tik prie tų išteklių, kurie yra būtini tiesioginių pareigų vykdymui.

28. Prieiga prie Registro galioja darbuotojui dirbant Fonde arba Ministerijoje, arba kol prieigos panaikinimo neinicijuoja darbuotojo tiesioginis vadovas. Naudotoją atleidžiant iš darbo (pareigų), prieiga prie Registro turi būti panaikinama nedelsiant.

29. Naudotoją priimant į darbą ar pareigas, darbuotojo tiesioginis vadovas užpildo prašymą, kuriame nurodo, kokia prieiga bus reikalinga. Šį prašymą pateikia Registro administratoriui. Prieigos suteikimo prašymai rašytine forma turi būti saugomi tol, kol Naudotojas dirba, ir metus po jo atleidimo iš darbo (pareigų).

30. Registro sistemose turi būti naudojama programinė įranga, skirta apsaugai nuo kenksmingo kodo (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir pan.):

30.1. antivirusinė programinė įranga Registro Naudotojų kompiuteriuose ir serveriuose;

30.2. programinės ugniasienės Registro Naudotojų kompiuteriuose ir serveriuose.

31. Apsaugai nuo kenksmingo kodo užtikrinti turi būti naudojamas nuolatinis Registro Naudotojų kompiuterių ir serverių operacinių sistemų ir taikomųjų programų atnaujinimas. Operacinių sistemų ir taikomųjų programų atnaujinimas atliekamas pagal gamintojo rekomendacijas.

32. Registro Naudotojų kompiuterių apsaugos priemonės turi būti valdomos (ugniasienių įjungimas ir konfigūravimas, antivirusinių programų atnaujinimas, operacinių sistemų atnaujinimas) centralizuotai.

33. Antivirusinių programų kenksmingi kodo aprašai turi būti atnaujinami ne rečiau kaip kartą per dieną.

34. Turi būti naudojama tik legali ir autorizuota programinė įranga.

35. Autorizuotos programinės įrangos sąrašą rengia Ministerijos Informacinių technologijų skyrius.

36. Siekiant nustatyti, ar Registro Naudotojai naudoja legalią ir autorizuotą programinę įranga, atliekamas programinės įrangos auditas. Auditą organizuoja Saugos įgaliotinis. Auditas atliekamas rizikos vertinimo metu, jo rezultatai įtraukiami į rizikos įvertinimo ataskaitą.

37. Registro duomenų perdavimo tinklas turi būti atskirtas nuo viešųjų telekomunikacijų tinklų ugniasiene.

38. Konfigūruojant duomenų perdavimo tinklo ugniasienes turi būti laikomasi principo „draudžiama viskas, išskyrus“, t.y., turi būti leidžiami tik būtini Registro veiklai prisijungimai prie duomenų perdavimo tinklo.

39. Už duomenų perdavimo tinklo ugniasienių priežiūrą, ugniasienės valdymo sistemos priežiūrą ir tinkamą ugniasienių sąranką yra atsakingas ugniasienės administratorius.

40. Duomenų perdavimo tinklo ugniasienių sąrankos aprašymą rengia ugniasienės administratorius. Sąrankos aprašymas yra saugomas pas ugniasienės administratorių.

41. Ministerijos ir Fondo kompiuteriai naudojami Registro Naudotojų tiesioginių pareigų atlikimui.

42. Kompiuteriais galima naudotis tik Ministerijos ar Fondo patalpose, išskyrus tuos atvejus, kai suderinus su IS administratoriumi suteikiamas leidimas kompiuteriais naudotis ne Ministerijos ar Fondo patalpose.

43. Registro Naudotojams, kuriems būtinas prisijungimas iš nutolusios darbo vietos, Ministerijos Informacinių technologijų skyriaus vedėjo sprendimu gali būti suteikiama nuotolinio prisijungimo galimybė.

44. Nuotolinis prisijungimas turi būti autorizuojamas. Autorizuotų nuotoliniam prisijungimui Naudotojų sąrašą rengia ir prižiūri Registro administratoriui. Sąrašas turi būti peržiūrimas ne rečiau kaip 2 kartus per metus.

45. Nuotolinio prisijungimo galimybė prie Registro sistemų suteikiama tik administratoriams ir Registro Naudotojams, kuriems tai yra būtina atliekant tiesiogines pareigas.

46. Techninis nuotolinio prisijungimo sprendimas turi užtikrinti ne žemesnį, nei naudojamą vidiniam prisijungimui, saugumo lygį.

47. Nuotolinio prisijungimo techninis sprendimas privalo užtikrinti:

47.1. elektroninių duomenų konfidencialumą;

47.2. elektroninių duomenų vientisumą.

48. Turi būti daromos atsarginės elektroninės informacijos kopijos, kurios turi būti laikomos atskiroje patalpoje, apsaugotos nuo nepalankių išorės veiksnių poveikio. Atsarginės duomenų kopijos turi būti daromos periodiškai, bet ne rečiau, kaip kartą per savaitę. Atstatymas iš atsarginių kopijų privalo būti išbandomas ne rečiau kaip kartą per metus. Duomenų atstatymo išbandymą organizuoja IS administratorius. Reikalavimai Registro sistemų funkcionalumo atstatymui ir prieinamumui:

48.1. turi būti užtikrintas pagrindinių sistemų funkcijų atkūrimas per 8 valandas nuo veiklos sutrikimo;

48.2. turi būti užtikrintas Registro sistemų prieinamumas ne mažiau kaip 90 procentų laiko darbo metu darbo dienomis.

IV. REIKALAVIMAI PERSONALUI

49. Registro objektų duomenis saugiai rinkti, apdoroti, sisteminti, kaupti, saugoti gali asmenys, susipažinę su Nuostatais ir kitais saugos politiką įgyvendinančiais dokumentais bei raštiškai sutikę laikytis šių teisės aktų reikalavimų.

50. Saugos įgaliotinis privalo išmanyti informacijos saugos užtikrinimo principus, savo darbe vadovautis Techniniais saugos reikalavimais ir Bendraisiais reikalavimais, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų duomenų tvarkymą, standartais ir kitais susijusiais dokumentais.

51. Administratoriai privalo išmanyti informacijos saugos principus, darbą su kompiuterių tinklais, mokėti užtikrinti jų saugumą, taip pat administruoti ir prižiūrėti duomenų bazes, turi būti susipažinę su Nuostatais. Personalui taikomi kvalifikaciniai reikalavimai nustatomi pareigybės aprašymuose.

52. Registro Naudotojai turi turėti kvalifikaciją (informacinių technologijų naudotojų kvalifikacijos kursai, pradinis saugaus darbo su duomenimis mokymas, ECDL (Europos kompiuterio naudotojo pažymėjimas) naudotojo sertifikatas ar pan.) ir patirties dirbant su atitinkamomis operacinėmis sistemomis, taikomosiomis programomis.

53. Saugos įgaliotinis Registro Naudotojams periodiškai, bet ne rečiau kaip kartą per metus, organizuoja mokymus elektroninės informacijos saugos klausimais.

V. REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

54. Saugos įgaliotinis organizuoja Registro Naudotojų rašytinį supažindinimą su Nuostatais ir saugos politiką įgyvendinančiais dokumentais bei atsakomybe už juose nustatytų reikalavimų nesilaikymą.

55. Saugos įgaliotinis informuoja Registro Naudotojus apie Nuostatų ir saugos politiką įgyvendinančių dokumentų pakeitimus.

VI. BAIGIAMOSIOS NUOSTATOS

56. Nuostatai yra privalomi visiems Registro Naudotojams, Saugos įgaliotiniui, IS administratoriui, vadovaujančiajai Registro tvarkymo įstaigai ir Registro tvarkymo įstaigai.

57. Saugos įgaliotinis, IS administratoriai, Registro Naudotojai, pažeidę Nuostatų ir saugos politiką įgyvendinančių dokumentų nuostatas, atsako įstatymų nustatyta tvarka.

_____