LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS
DĖL LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRO 2009 M. RUGSĖJO 29 D. ĮSAKYMO NR. V-819 „DĖL MIRTIES ATVEJŲ IR JŲ PRIEŽASČIŲ VALSTYBĖS REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO

2018 m. rugpjūčio 30 d. Nr. V-970
Vilnius

P a k e i č i u Lietuvos Respublikos sveikatos apsaugos ministro 2009 m. rugsėjo 29 d. įsakymą Nr. V-819 „Dėl Mirties atvejų ir jų priežasčių valstybės registro duomenų saugos nuostatų patvirtinimo“:

1. Pakeičiu preambulę ir ją išdėstau taip:

„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, 19 punktu ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“, 5 ir 7 punktais:“.

2. Pakeičiu nurodytu įsakymu patvirtintus Mirties atvejų ir jų priežasčių valstybės registro duomenų saugos nuostatus ir juos išdėstau nauja redakcija (pridedama).

Sveikatos apsaugos ministras Aurelijus Veryga

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2018 m. liepos 16 d. raštu Nr. (4.2)6K-425

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos
ministro 2009 m. rugsėjo 29 d.
įsakymu Nr. V-819
(Lietuvos Respublikos sveikatos apsaugos
ministro 2018 m. rugpjūčio 30 d. įsakymo
Nr. V-970
redakcija)

MIRTIES ATVEJŲ IR JŲ PRIEŽASČIŲ VALSTYBĖS REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Mirties atvejų ir jų priežasčių valstybės registro duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Mirties atvejų ir jų priežasčių valstybės registro (toliau – Registras) elektroninės informacijos saugos politiką ir kibernetinio saugumo politiką (toliau – elektroninės informacijos saugos politika), organizacines, technines, programines, teisines ir kitas priemones, užtikrinančias saugų Registro elektroninės informacijos tvarkymą.

2. Šiuose Saugos nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame 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“ (toliau – Bendrųjų saugos reikalavimų aprašas), Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei struktūrai ir valstybės informaciniams ištekliams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei struktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas), Mirties atvejų ir jų priežasčių valstybės registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2009 m. liepos 8 d. nutarimu Nr. 709 „Dėl Mirties atvejų ir jų priežasčių valstybės registro nuostatų patvirtinimo (toliau – Registro nuostatai), vartojamas sąvokas.

3. Registro elektroninės informacijos saugos ir kibernetinio saugumo (toliau – elektroninės informacijos sauga) tikslas – užtikrinti Registro elektroninės informacijos konfidencialumą, prieinamumą ir vientisumą ir sudaryti sąlygas saugiai automatiniu būdu tvarkyti Registro elektroninę informaciją.

4. Elektroninės informacijos saugos politika įgyvendinama pagal Registro valdytojo tvirtinamus saugos politiką įgyvendinančius dokumentus:

4.1. Mirties atvejų ir jų priežasčių valstybės registro saugaus elektroninės informacijos tvarkymo taisykles;

4.2. Mirties atvejų ir jų priežasčių valstybės registro naudotojų administravimo taisykles;

4.3. Mirties atvejų ir jų priežasčių valstybės registro veiklos tęstinumo valdymo planą.

5. Registro elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

5.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų Registro duomenų saugai užtikrinti, įgyvendinimas ir šių priemonių kontrolė;

5.2. Registre tvarkomų asmens duomenų apsauga;

5.3. Registro veikos tęstinumo užtikrinimas.

6. Saugos nuostatų reikalavimai taikomi:

6.1. Registro valdytojui – Lietuvos Respublikos sveikatos apsaugos ministerijai, Vilniaus g. 33, Vilnius;

6.2. Registro tvarkytojui – Higienos institutui, Didžioji g. 22, Vilnius;

6.3. Registro naudotojams;

6.4. Registro saugos įgaliotiniui;

6.5. Registro duomenų valdymo įgaliotiniui;

6.6. Registro administratoriui;

6.7. kibernetinio saugumo vadovui.

7. Už elektroninės informacijos saugą pagal kompetenciją atsako Registro valdytojas ir Registro tvarkytojas.

8. Registro naudotojai, duomenų valdymo įgaliotinis ir administratorius privalo įsipareigoti saugoti duomenų ir informacijos paslaptį bei pasirašyti konfidencialumo pasižadėjimą. Įsipareigojimas saugoti duomenų ir informacijos paslaptį galioja ir nutraukus su Registru susijusią veiklą.

9. Registro valdytojas atlieka Registro nuostatuose nustatytas funkcijas, taip pat:

9.1. tvirtina saugos politiką įgyvendinančius dokumentus, kitus dokumentus, susijusius su elektroninės informacijos sauga, ir jų pakeitimus;

9.2. nagrinėja Registro tvarkytojo pasiūlymus dėl Registro elektroninės informacijos saugos priemonių tobulinimo ir priima sprendimus dėl jų finansavimo;

9.3. priima sprendimus dėl techninių ir programinių priemonių, būtinų Registro elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

9.4. vykdo kitas Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Bendrųjų saugos reikalavimų apraše, Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše, Registro nuostatuose bei kituose teisės aktuose nustatytas funkcijas, susijusias su elektroninės informacijos sauga.

10. Registro tvarkytojas atlieka Registro nuostatuose nustatytas funkcijas, taip pat:

10.1. pagal kompetenciją atsako už Registro elektroninės informacijos tvarkymo teisėtumą ir saugą;

10.2. įgyvendina tinkamas organizacines ir technines priemones, skirtas elektroninei informacijai apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

10.3. pagal kompetenciją įgyvendina Registro saugos dokumentų ir kitų saugos politiką įgyvendinančių teisės aktų reikalavimus;

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

10.5. užtikrina, kad Registro naudotojai, turintys teisę naudotis Registro elektronine informacija, laikytųsi reikalavimų, nustatytų Registro saugos dokumentuose;

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

10.7. užtikrina saugią Registro sąveiką su kitomis informacinėmis sistemomis ir registrais;

10.8. teikia pasiūlymus Registro valdytojui dėl Registro techninių ir programinių priemonių, būtinų Registro elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo, organizuoja jų įdiegimą ir modernizavimą;

10.9. skiria Registro duomenų valdymo įgaliotinį, Registro saugos įgaliotinį ir Registro administratorių;

10.10. atlieka kitas Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Bendrųjų saugos reikalavimų apraše, Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše, Registro nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

11. Registro saugos įgaliotinio funkcijos ir atsakomybė:

11.1. koordinuoja ir prižiūri Registro elektroninės informacijos saugos politikos įgyvendinimą;

11.2. teikia Registro tvarkytojo vadovui pasiūlymus dėl:

11.2.1. Registro administratoriaus paskyrimo;

11.2.2. Registro informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

11.3. teikia pasiūlymus Registro valdytojui dėl Registro saugos dokumentų priėmimo, keitimo ar pripažinimo netekus galios;

11.4. koordinuoja Registro elektroninės informacijos saugos incidentų tyrimą;

11.5. organizuoja Registro rizikos įvertinimą ir parengia rizikos įvertinimo ataskaitą;

11.6. teikia Registro administratoriui ir Registro naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos politikos įgyvendinimu;

11.7. turi teisę pagal savo įgaliojimus duoti privalomus vykdyti nurodymus ir pavedimus ir kitiems Registro tvarkytojo darbuotojams, jeigu tai būtina saugos politikai įgyvendinti;

11.8. supažindina Registro administratorių ir Registro naudotojus su Registro saugos politiką įgyvendinančių dokumentų reikalavimais ir atsakomybe už reikalavimų nesilaikymą, organizuoja Registro naudotojų mokymą elektroninės informacijos saugos klausimais, informuoja juos apie elektroninės informacijos saugos problemas;

11.9. atlieka kitas Bendrųjų saugos reikalavimų apraše, Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše, Registro nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

12. Registro administratoriaus funkcijos ir atsakomybė:

12.1. atsako už Registro techninės ir programinės įrangos funkcionavimą;

12.2. diegia ir prižiūri programinę įrangą, reikalingą Registro naudotojų funkcijoms vykdyti;

12.3. suteikia teisę Registro naudotojams naudotis elektronine informacija, reikalinga jų funkcijoms atlikti;

12.4. užtikrina registro komponentų (kompiuterių, tarnybinių stočių, operacinių sistemų, taikomųjų programų, duomenų bazės valdymo sistemų, ugniasienių, įsilaužimų aptikimo sistemų ir kt.) tinkamą veikimą ir priežiūrą, pagal kompetenciją nustato Registro pažeidžiamas vietas;

12.5. dalyvauja vykdant saugumo reikalavimų įgyvendinimo stebėseną;

12.6. pagal kompetenciją teikia Registro tvarkytojo vadovui pasiūlymus dėl Registro palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

12.7. informuoja Registro saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikia pasiūlymus dėl elektroninės informacijos saugos incidentų pašalinimo;

12.8. atsako už Registro duomenų bazės atsarginių kopijų darymą;

12.9. atlieka kitas Bendrųjų saugos reikalavimų apraše, Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše, Registro nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

13. Kibernetinio saugumo vadovas vykdo kibernetinio saugumo organizavimo ir užtikrinimo funkcijas, nustatytas Lietuvos Respublikos kibernetinio saugumo įstatyme, Kibernetinio saugumo reikalavimų apraše ir kituose kibernetinį saugumą reglamentuojančiuose teisės aktuose.

14. Teisės aktai, kuriais vadovaujantis tvarkoma Registro elektroninė informacija ir užtikrinama jos sauga:

14.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

14.2. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

14.3. Lietuvos Respublikos kibernetinio saugumo įstatymas;

14.4. Bendrųjų saugos reikalavimų aprašas;

14.5. Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas, patvirtintas 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“ (toliau – Klasifikavimo gairių aprašas);

14.6. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti 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“;

14.7. Mirties atvejų ir jų priežasčių valstybės registro nuostatai;

14.8. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas;

14.9. Lietuvos standartai ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, nustatantys saugų elektroninės informacijos tvarkymą;

14.10. kiti teisės aktai, reglamentuojantys elektroninės informacijos tvarkymo teisėtumą ir elektroninės informacijos saugos valdymą valstybės institucijose.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

15. Registre tvarkoma elektroninė informacija priskiriama vidutinės svarbos informacijos kategorijai, vadovaujantis Klasifikavimo gairių aprašo 9.1 ir 9.2 papunkčiuose nustatytais kriterijais.

16. Registras priskiriamas trečiajai kategorijai, vadovaujantis Klasifikavimo gairių aprašo 12.3 papunkčio nuostatomis, atsižvelgiant į Registre tvarkomos elektroninės informacijos svarbos kategoriją.

17. Registro saugos priemonės parenkamos įvertinus galimus rizikos veiksnius elektroninės informacijos vientisumui, konfidencialumui ir prieinamumui.

18. Registro rizikos veiksniams vertinti naudojama Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistema (toliau – ARSIS). Kartu su pagrindiniu Registro rizikos vertinimu organizuojamas ir atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos Registro kibernetiniam saugumui, vertinimas.

19. Pagrindinės Registro rizikos mažinimo priemonės išdėstomos rizikos įvertinimo ataskaitoje, kurią kasmet iki gruodžio 31 d. rengia Registro saugos įgaliotinis, įvertinęs galinčius turėti įtakos elektroninės informacijos saugai rizikos veiksnius, iš kurių svarbiausi 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, netinkamas veikimas ir kita);

19.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo 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. Elektroninės informacijos saugos būklė gerinama techninėmis, programinėmis ir organizacinėmis saugos priemonėmis, kurios pasirenkamos atsižvelgiant į Registro valdytojo skiriamus išteklius, vadovaujantis šiais principais:

20.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

20.2. saugos priemonės diegimo kaina turi atitikti saugomos elektroninės informacijos vertę;

20.3. esant galimybei, turi būti įdiegiamos prevencinės elektroninės informacijos saugos priemonės.

21. Registro valdytojas tvirtina Registro tvarkytojo parengtą rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

22. Siekiant įvertinti saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, kartą per dvejus metus organizuojamas Registro informacinių technologijų saugos reikalavimų atitikties vertinimas.

23. Registro informacinių technologijų saugos reikalavimų atitikčiai vertinti naudojama ARSIS.

24. Atlikus Registro informacinių technologijų saugos reikalavimų atitikties vertinimą, rengiama Registro saugos atitikties vertinimo ataskaita, kurią tvirtina Registro tvarkytojas.

25. Registro rizikos įvertinimo ataskaitos ir rizikos valdymo priemonių plano, Registro saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas Registro tvarkytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų patvirtinimo pateikia ARSIS Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2012 m. spalio 16 d. įsakymu Nr. 1V-740 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

26. Programinės įrangos, skirtos Registrą apsaugoti nuo kenksmingosios programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir panašiai), naudojimo nuostatos ir jos atnaujinimo reikalavimai:

26.1. Registro tarnybinėse stotyse ir kompiuterizuotose darbo vietose turi būti naudojamos centralizuotai valdomos kenksmingosios programinės įrangos aptikimo priemonės, nuolat ieškančios ir blokuojančios kenksmingąją programinę įrangą, kurios turi būti reguliariai atnaujinamos automatiniu būdu ne rečiau kaip kartą per 24 valandas;

26.2. apsaugai naudojama programinė įranga privalo automatiškai elektroniniu paštu informuoti Registro administratorių apie kompiuterizuotas darbo vietas ir tarnybines stotis, kuriose apsaugos sistema netinkamai funkcionuoja, yra išjungta arba neatsinaujino per 24 valandas;

26.3. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

27. Programinės įrangos, įdiegtos tarnybinėse stotyse ir kompiuterizuotose darbo vietose, naudojimo nuostatos:

27.1. Registro darbui turi būti naudojama tik legali, Registro funkcijoms vykdyti būtina programinė įranga;

27.2. programinė įranga atnaujinama laikantis gamintojo reikalavimų;

27.3. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka Registro administratorius;

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

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

29. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kita) pagrindinės naudojimo nuostatos:

29.1. Registro elektroninės informacijos perdavimo tinklas nuo viešųjų telekomunikacijų tinklų (interneto) turi būti atskirti ugniasienėmis, DOS ir DDOS atakų prevencijai skirta įranga bei įsilaužimų aptikimo ir prevencijos įranga;

29.2. Registro tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių Registro naudotojų kompiuterinę įrangą nuo kenksmingo kodo.

30. Leistinos kompiuterių naudojimo ribos:

30.1. stacionarieji ir nešiojamieji Registro naudotojų kompiuteriai turi būti naudojami tik tiesioginėms pareigoms atlikti. Iš kompiuterių, kurie perduodami remontuoti ar techninei priežiūrai atlikti, turi būti pašalinti visi Registro duomenys ir Registro informacija;

30.2. nešiojamieji kompiuteriai gali būti naudojami tik suvestiniams (viešiems) Registro duomenims ir negali būti naudojami Registro duomenims registruoti, kaupti ir apdoroti;

30.3. nešiojamuosiuose kompiuteriuose turi būti naudojamas įjungimo slaptažodis;

30.4. Registro naudotojai privalo naudotis visomis saugumo priemonėmis, siekdami apsaugoti kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo, nenaudojami nešiojamieji kompiuteriai turi būti saugomi saugioje vietoje.

31. Metodai, kuriais užtikrinamas saugus Registro elektroninės informacijos teikimas ir (ar) gavimas:

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

31.2. elektroninė informacija iš susijusių registrų gaunama tik pagal duomenų teikimo ir gavimo sutartyse nustatytas perduodamų duomenų specifikacijas, perdavimo sąlygas ir tvarką;

31.3. prieigos prie Registro elektroninės informacijos teises gali suteikti tik Registro administratorius. Registro naudotojams suteikiamos tik jų funkcijoms vykdyti būtinos teisės;

31.4. prieiga prie Registro elektroninės informacijos leidžiama tik per registravimosi slaptažodžių sistemą. Prieigos prie Registro elektroninės informacijos valdymas apibrėžtas Registro naudotojų administravimo taisyklėse;

31.5. pasibaigus Registro naudotojo darbo sutarčiai, teisė naudotis Registro elektronine informacija turi būti panaikinta. Registro naudotojui prieiga prie Registro turi būti ribojama ar sustabdoma, kai vyksta Registro naudotojo veiklos tyrimas, naudotojas yra ilgalaikėse atostogose arba keičiasi jo atliekamos ir (ar) pareigybės aprašyme nurodytos funkcijos.

32. Registro naudotojai, pastebėję saugos dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai Registro administratoriui ar Registro saugos įgaliotiniui.

33. Registro veiklos tęstinumui ir funkcionalumui užtikrinti elektroninė informacija automatiniu būdu, esant aktyviai Registro duomenų bazei, kopijuojama kiekvieną dieną. Elektroninės informacijos kopijos turi būti saugomos kitoje patalpoje, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota.

34. Turi būti užtikrintas saugos incidentų, įvykusių Registre, registravimas, valdymas ir tyrimas Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo ir Registro veiklos tęstinumo valdymo plano nustatyta tvarka:

34.1. registruojami Registre įvykę saugos incidentai ir nedelsiant į juos reaguojama, techninėmis ir programinėmis priemonėmis pagal kompetenciją saugos incidentai valdomi, tiriami ir šalinami bei atkuriama Registro veikla;

34.2. Nacionaliniam kibernetinio saugumo centrui ir kitoms atsakingoms institucijoms pagal kompetenciją pranešama apie įvykusius saugos incidentus, jų vertinimą ir suvaldymą.

35. Ne rečiau kaip kartą per mėnesį turi būti atliekama ugniasienių užfiksuotų įvykių analizė ir pastebėtos neatitiktys saugumo reikalavimams nedelsiant šalinamos.

36. Perkant paslaugas, darbus ar įrangą, susijusius su Registru, jo projektavimu, kūrimu, diegimu, modernizavimu, priežiūra, palaikymu, saugos užtikrinimu, auditavimu, elektroninės informacijos perdavimo tinklais, taip pat kitus, suteikiančius teisę ir galimybę prieiti prie elektroninės informacijos, pirkimo dokumentuose turi būti nustatyta, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas privalo laikytis Registro saugos dokumentuose nustatytų reikalavimų ir užtikrinti teikiamų paslaugų, vykdomų darbų ar tiekiamos įrangos atitiktį Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo reikalavimams.

37. Į paslaugų pirkimo sutartį turi būti įtraukta nuostata, įpareigojanti paslaugų teikėjo darbuotojus pasirašyti konfidencialumo pasižadėjimą neatskleisti tretiesiems asmenims jokios informacijos, gautos vykdant šią sutartį, išskyrus tiek, kiek būtina sutarčiai vykdyti, nenaudoti konfidencialios informacijos asmeniniams ar trečiųjų asmenų poreikiams laikantis principo, kad visa paslaugų teikėjui suteikta informacija yra konfidenciali, nebent raštu patvirtinama, kad tam tikra pateikta informacija nėra konfidenciali.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

38. Registro saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis Bendrųjų saugos reikalavimų aprašu, kitais Lietuvos Respublikos teisės aktais ir Europos Sąjungos teisės aktų nuostatomis, reglamentuojančiomis elektroninės informacijos saugą, kibernetinę saugą, tobulinti kvalifikaciją elektroninės informacijos saugos srityje.

39. Registro saugos įgaliotiniu, Registro administratoriumi ir kibernetinio saugumo vadovu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

40. Registro administratorius pagal kompetenciją privalo išmanyti elektroninės informacijos saugos, kibernetinio saugumo užtikrinimo principus, mokėti užtikrinti Registro duomenų saugą, darbo su duomenų perdavimo tinklais principus, administruoti ir prižiūrėti Registro duomenų bazę, gebėti užtikrinti techninės ir programinės įrangos nepertraukiamą funkcionavimą, stebėti jos veikimą, atlikti jos profilaktinę priežiūrą, būti susipažinęs su Registro saugos dokumentais, pagal kompetenciją ir kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą.

41. Registro saugos įgaliotinio, kibernetinio saugumo vadovo, Registro naudotojų ir Registro administratoriaus mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo dažnumo reikalavimai:

41.1. Registro saugos įgaliotiniui, kibernetinio saugumo vadovui, Registro naudotojams ir Registro administratoriui turi būti organizuojami mokymai elektroninės informacijos saugos klausimais;

41.2. Registro naudotojams turi būti įvairiais būdais (pavyzdžiui, priminimai elektroniniu paštu, teminių renginių organizavimas, atmintinės naujiems Registro naudotojams ir Registro administratoriui ir panašiai) primenama apie elektroninės informacijos saugos problemas;

41.3. mokymai elektroninės informacijos saugos klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į prioritetines elektroninės informacijos saugos užtikrinimo kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), Registro saugos įgaliotinio, kibernetinio saugumo vadovo, naudotojų ar administratoriaus poreikius;

41.4. mokymai gali būti vykdomi tiesioginiu (pavyzdžiui, paskaitos, seminarai, konferencijos ir kiti teminiai renginiai) ar nuotoliniu būdu (pavyzdžiui, vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir panašiai);

41.5. Registro naudotojų ir Registro administratoriaus mokymus gali vykdyti Registro saugos įgaliotinis ar kitas Registro valdytojo ar Registro tvarkytojo darbuotojas, išmanantis elektroninės informacijos saugos užtikrinimo principus, arba elektroninės informacijos saugos mokymų paslaugų teikėjas. Registro saugos įgaliotinio ir kibernetinio saugumo vadovo mokymus gali vykdyti tik aukštos kvalifikacijos elektroninės informacijos saugos mokymų paslaugų teikėjas;

41.6. Registro naudotojų mokymai turi būti organizuojami periodiškai, ne rečiau kaip kartą per dvejus metus. Registro saugos įgaliotinio, kibernetinio saugumo vadovo ir Registro administratoriaus mokymai turi būti organizuojami pagal poreikį. Už mokymų organizavimą atsakingas Registro saugos įgaliotinis ar kitas Registro tvarkytojo paskirtas darbuotojas.

42. Registro naudotojai privalo turėti darbo kompiuteriu įgūdžių, mokėti tvarkyti Registro duomenis Registro nuostatų nustatyta tvarka, būti susipažinę su Registro saugos dokumentais ir pasirašę pasižadėjimus saugoti konfidencialią elektroninę informaciją.

V SKYRIUS
REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

43. Tvarkyti Registro duomenis ir gauti informaciją gali tik Registro naudotojai, susipažinę su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais, kuriais vadovaujamasi tvarkant elektroninę informaciją, ir raštu pasirašę pasižadėjimus saugoti asmens duomenų paslaptį.

44. Už Registro naudotojų supažindinimą su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais bei atsakomybe už šių reikalavimų nesilaikymą atsakingas yra Registro saugos įgaliotinis. Pakartotinai su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais Registro naudotojai supažindinami tik iš esmės jiems pasikeitus.

45. Saugos nuostatai skelbiami Registro tvarkytojo interneto svetainėje.

46. Registro naudotojai, pažeidę Registro saugos dokumentų reikalavimus, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

_____