LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS DĖL LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRO 2009 M. SPALIO 8 D. ĮSAKYMO NR. V-850 „DĖL LIETUVOS RESPUBLIKOS PROFESINIŲ LIGŲ VALSTYBĖS REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO

2014 m. rugsėjo 25 d. Nr. V-988
Vilnius

P a k e i č i u Lietuvos Respublikos sveikatos apsaugos ministro 2009 m. spalio 8 d. įsakymą Nr. V-850 „Dėl Lietuvos Respublikos profesinių ligų valstybės registro duomenų saugos nuostatų patvirtinimo“ ir išdėstau jį nauja redakcija:

„LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS DĖL LIETUVOS RESPUBLIKOS PROFESINIŲ LIGŲ VALSTYBĖS REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

Vadovaudamasi Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimo Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ 2 punktu:

1. T v i r t i n u Lietuvos Respublikos profesinių ligų valstybės registro duomenų saugos nuostatus (pridedama).

2. P a v e d u Higienos instituto direktoriui per 5 mėnesius nuo šio įsakymo įsigaliojimo dienos:

2.1. paskirti Lietuvos Respublikos profesinių ligų valstybės registro duomenų valdymo įgaliotinį, saugos įgaliotinį ir Registro administratorių;

2.2. pateikti Lietuvos Respublikos sveikatos apsaugos ministrui tvirtinti:

2.2.1. Lietuvos Respublikos profesinių ligų valstybės registro naudotojų administravimo taisyklių projektą;

2.2.2. Lietuvos Respublikos profesinių ligų valstybės registro saugaus elektroninės informacijos tvarkymo taisyklių projektą;

2.2.3. Lietuvos Respublikos profesinių ligų valstybės registro veiklos tęstinumo valdymo plano projektą.“

Sveikatos apsaugos ministrė Rimantė Šalaševičiūtė

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2014 m. liepos 22 d. raštu Nr. 1D-5356 (52)

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro 2009 m. spalio 8 d. įsakymu Nr. V-850
(Lietuvos Respublikos sveikatos apsaugos ministro 2014 m. rugsėjo 25 d. įsakymo Nr. V- 988 redakcija)

LIETUVOS RESPUBLIKOS PROFESINIŲ LIGŲ VALSTYBĖS REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos profesinių ligų valstybės registro (toliau – Registras) duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Registro juridinių ir fizinių asmenų, kuriems taikomi šie Saugos nuostatai, funkcijas ir atsakomybę, elektroninės informacijos saugos valdymą, organizacinius ir techninius reikalavimus.

2. Šiuose Saugos nuostatuose vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, Lietuvos Respublikos profesinių ligų valstybės registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 1994 m. lapkričio 30 d. nutarimu Nr. 1198 (toliau – Registro nuostatai), kituose teisės aktuose ir Lietuvos Respublikos standartuose LST ISO/IEC 27002:2009 ir LST ISO/IEC 27001:2006.

3. Registro elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

3.1. techninės ir programinės įrangos, naudojamos Registro elektroninei informacijai tvarkyti, priežiūra ir kontrolė;

3.2. prieigos prie Registro elektroninės informacijos kontrolė;

3.3. Registro elektroninės informacijos konfidencialumo, vientisumo ir reikalaujamo prieinamumo lygio užtikrinimas;

3.4. saugaus kompiuterinio ryšio, priimant ir perduodant informaciją elektroniniu paštu, užtikrinimas;

3.5. Registro duomenų konfidencialumo užtikrinimas.

4. Registro elektroninės informacijos saugumo užtikrinimo tikslas – sudaryti sąlygas saugiai automatizuotu būdu saugoti ir tvarkyti Registro elektroninę informaciją, užtikrinti jos konfidencialumą, vientisumą ir prieinamumą.

5. Saugos nuostatai taikomi:

5.1. Registro valdytojai – Lietuvos Respublikos sveikatos apsaugos ministerijai, Vilniaus g. 33, LT-01506 Vilnius;

5.2. Registro tvarkytojui – Higienos institutui, Didžioji g. 22, LT-01128 Vilnius;

5.3. Registro naudotojams;

5.4. Registro saugos įgaliotiniui;

5.5. Registro administratoriui.

6. Registro valdytojas:

6.1. pagal kompetenciją atsako už saugos politikos formavimą, jos įgyvendinimo organizavimą ir priežiūrą;

6.2. tvirtina Registro saugos nuostatus, saugaus elektroninės informacijos tvarkymo taisykles, veiklos tęstinumo valdymo planą, naudotojų administravimo taisykles (toliau visi kartu – saugos dokumentai) ir kitus teisės aktus, kuriuose reglamentuojamas Registro tvarkymo teisėtumas ir Registro elektroninės informacijos sauga;

6.3. koordinuoja Registro tvarkytojo darbą;

6.4. analizuoja Registro tvarkytojo pateiktus pasiūlymus, priima sprendimus dėl Registro techninių ir programinių priemonių, būtinų Registro elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

6.5. skiria Registro duomenų valdymo įgaliotinį, Registro saugos įgaliotinį ir Registro administratorių arba paveda juos skirti Registro tvarkytojui;

6.6. atlieka kitas Registro nuostatų ir saugos dokumentų jam priskirtas funkcijas.

7. Registro tvarkytojas:

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

7.2. 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;

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

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

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

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

7.7. užtikrina saugią registro sąveiką su kitomis informacinėmis sistemomis ir registrais;

7.8. 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;

7.9. Registro valdytojo vadovo pavedimu skiria Registro duomenų valdymo įgaliotinį, Registro saugos įgaliotinį ir Registro administratorių;

7.10. atlieka kitas Registro valdytojo pavestas, Registro nuostatų, saugos dokumentų ir kitų saugos politiką įgyvendinančių teisės aktų jam priskirtas funkcijas.

8. Registro saugos įgaliotinis:

8.1. atsako už tinkamą Registro elektroninės informacijos saugos priemonių įgyvendinimą;

8.2. teikia Registro tvarkytojo vadovui siūlymus dėl:

8.2.1. Registro administratoriaus paskyrimo ir reikalavimų administratoriui nustatymo;

8.2.2. Registro saugos atitikties vertinimo atlikimo;

8.3. teikia Registro valdytojui pasiūlymus dėl Registro saugos dokumentų priėmimo arba keitimo;

8.4. koordinuoja elektroninės informacijos saugos incidentų, įvykusių Registre, tyrimą;

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

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

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

8.8. supažindina Registro administratorių ir Registro naudotojus su Registro saugos dokumentų reikalavimais ir atsakomybe už reikalavimų nesilaikymą, organizuoja Registro

naudotojų mokymą elektroninės informacijos saugos klausimais, informuoja juos apie elektroninės informacijos saugos problemas;

8.9. atlieka kitas Registro tvarkytojo vadovo pavestas, Registro saugos dokumentų ir kitų saugos politiką įgyvendinančių teisės aktų jam priskirtas funkcijas.

9. Registro administratorius:

9.1. atsako už Registro techninės ir programinės įrangos funkcionavimą;

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

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

9.4. 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;

9.5. dalyvauja vykdant saugumo reikalavimų įgyvendinimo stebėseną;

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

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

9.8. atsako už Registro duomenų bazės atsarginių kopijų darymą;

9.9. atlieka kitas Registro tvarkytojo vadovo, saugos įgaliotinio pavestas, Registro saugos dokumentų ir kitų saugos politiką įgyvendinančių teisės aktų jam priskirtas funkcijas.

10. Teisės aktai, kuriais vadovaujamasi tvarkant Registro elektroninę informaciją ir užtikrinant jos saugumą:

10.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

10.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

10.3. Lietuvos Respublikos dokumentų ir archyvų įstatymas;

10.4. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

10.5. 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“;

10.6. Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtinti Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms patvirtinimo“ (toliau – Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms“);

10.7. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

10.8. Lietuvos standartai LST ISO/IEC 27002:2009, LST ISO/IEC 27001:2006, kiti Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, nustatantys saugų elektroninės informacijos tvarkymą;

10.9. kiti teisės aktai, reglamentuojantys elektroninės informacijos saugumo politiką, jos tvarkymo teisėtumą ir saugos valdymą valstybės institucijose.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

11. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 4 ir 5 punktais:

11.1. Registre tvarkoma elektroninė informacija pagal svarbą priskiriama prie svarbios elektroninės informacijos kategorijos, priskyrimo prie šios kategorijos sistemų kriterijai: Registro elektroninės informacijos praradimas gali turėti neigiamų padarinių gyventojų sveikatos apsaugai, taip pat gali sutrikdyti kelių institucijų veiklą ar viešųjų paslaugų teikimą daugiau kaip vienai dienai;

11.2. Registras priskiriamas prie antros kategorijos informacinių sistemų, priskyrimo prie šios kategorijos sistemų kriterijus – Registre apdorojama svarbi elektroninė informacija.

12. Vadovaujantis Bendrųjų reikalavimų organizacinių ir techninių duomenų saugumo priemonių 7 punktu, Registre tvarkomi asmens duomenys priskiriami prie trečiojo asmens duomenų saugumo lygio.

13. Registro saugos įgaliotinis, vadovaudamasis Lietuvos Respublikos vidaus reikalų ministerijos metodine priemone „Rizikos analizės vadovas“, kasmet organizuoja Registro rizikos įvertinimą. Pasikeitus Registro duomenų bazės struktūrai (sistemos pakeitimai, papildymas naujomis taikomosiomis programomis, taikomųjų programų šalinimas ir kt.) ar nustačius naujų rizikos veiksnių, gali būti organizuojamas neeilinis registro duomenų saugos rizikos įvertinimas.

14. Registro rizikos vertinimo metu įvertinami rizikos veiksniai, galintys turėti įtakos Registro elektroninės informacijos saugai, jų galima žala, pasireiškimo tikimybė, galimi rizikos valdymo būdai. Svarbiausieji rizikos veiksniai yra šie:

14.1. 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);

14.2. 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);

14.3. 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.

15. Registro rizikos veiksniams vertinti naudojama penkiabalė rizikos vertinimo sistema, pagal kurią, nustačius rizikos veiksnių tikimybę ir poveikį, apskaičiuojamas rizikos laipsnis:

15.1. rizikos laipsnis nuo 1 iki 6 – maža rizika;

15.2. rizikos laipsnis nuo 8 iki 12 – vidutinė rizika;

15.3. rizikos laipsnis nuo 15 iki 25 – didelė rizika.

16. Kuo didesnė rizikos veiksnio tikimybė ir jo poveikis, tuo rizikos laipsnis aukštesnis. Rizikos veiksniams, kuriems nustatytas aukštas rizikos laipsnis, būtina skirti didžiausią dėmesį, parenkant ir įgyvendinant tinkamas rizikos mažinimo priemones.

17. Registro rizikos įvertinimo rezultatai ir priemonės rizikos veiksniams išvengti išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama Registro tvarkytojo vadovui.

18. Elektroninės informacijos saugos priemonių parinkimo principai:

18.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

18.2. saugos priemonės diegimo kaina turi būti adekvati saugomos elektroninės informacijos vertei;

18.3. kur galima, turi būti įdiegiamos prevencinės informacijos saugos priemonės;

18.4. Registro veiklos tęstinumo ir elektroninės informacijos saugos užtikrinimas patiriant kuo mažiau išlaidų.

19. Siekiant įvertinti Registro saugos dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, kartą per metus organizuojamas informacinių technologijų saugos atitikties vertinimas.

20. Atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama Registro tvarkytojo vadovui.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

21. Programinės įrangos, skirtos Registrui nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.) apsaugoti, naudojimo nuostatos ir atnaujinimo reikalavimai:

21.1. Registro tarnybinėse stotyse ir kompiuterizuotose darbo vietose turi būti įdiegta centralizuotai valdoma programinė įranga, skirta Registrui nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.) apsaugoti, kuri turi atsinaujinti automatiniu būdu ne rečiau kaip kartą per 24 valandas;

21.2. 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;

21.3. apsaugai naudojama programinė įranga turi turėti apsaugos mechanizmus, blokuojančius kenkimo programų bandymus panaikinti apsaugas nuo kenkimo programų.

22. Programinės įrangos, įdiegtos kompiuteriuose ir tarnybinėse stotyse, naudojimo nuostatos:

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

22.2. programinė įranga turi būti nuolatos atnaujinama laikantis gamintojo reikalavimų;

22.3. programinės įrangos diegimą, šalinimą ir konfigūravimą gali atlikti tik Registro administratorius;

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

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

23.1. Registro elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienes, ugniasienių įvykių žurnalai turi būti reguliariai analizuojami;

23.2. Registro programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. SQL injection), XSS (angl. Cross-site scripting), atkirtimo nuo paslaugos (angl. DOS), dedikuoto atkirtimo nuo paslaugos (angl. DDOS);

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

24. Leistinos kompiuterių naudojimo ribos:

24.1. 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;

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

24.3. nešiojamuosiuose kompiuteriuose turi būti naudojamas įjungimo slaptažodis;

24.4. Registro duomenų naudotojai privalo naudotis visomis saugumo priemonėmis, siekdami apsaugoti kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo;

24.5. kai nešiojamieji kompiuteriai nenaudojami, jie turi būti saugomi saugioje vietoje;

24.6. Registro tvarkytojo stacionarų kompiuterį prijungti prie Registro kompiuterių tinklo gali tik Registro administratorius.

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

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

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

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

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

25.5. 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.

26. Registro veiklos tęstinumui ir funkcionalumui užtikrinti elektroninė informacija automatiniu būdu kopijuojama kas 24 valandas. Kartą per savaitę daromos atsarginės elektroninės informacijos kopijos, kurios turi būti saugomos kitoje patalpoje nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

27. Saugos įgaliotinis turi išmanyti elektroninės informacijos saugos užtikrinimo principus, tobulinti kvalifikaciją elektroninės informacijos saugos srityje, savo darbe vadovautis Registro saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų duomenų tvarkymą.

28. Saugos įgaliotiniu 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, elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

29. Registro administratorius privalo išmanyti darbą su duomenų perdavimo tinklais, mokėti užtikrinti jų saugą, administruoti ir prižiūrėti duomenų bazes, turi būti susipažinęs su Registro nuostatais, Registro saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų duomenų tvarkymą.

30. 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 informaciją apie asmens duomenis (toliau – pasižadėjimai).

31. Registro elektroninę informaciją tvarkyti ir teikti Registro nuostatuose nurodytiems Registro duomenų gavėjams gali asmenys, turintys pagrindinius darbo su kompiuteriu įgūdžius, mokantys tvarkyti registro duomenis Registro nuostatuose, Registro funkcinėje sistemos specifikacijoje, Registro naudojimo ir administravimo instrukcijoje nurodyta tvarka bei susipažinę su Saugos nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų reikalavimais.

32. Saugos įgaliotinis ne rečiau kaip kartą per dvejus metus inicijuoja Registro naudotojų mokymą elektroninės informacijos saugos klausimais, periodiškai įvairiais būdais primena apie saugumo problemas (pvz., pranešimai elektroniniu paštu, naujų darbuotojų instruktavimas ir pan.).

V SKYRIUS
REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

33. Tvarkyti Registro duomenis ir gauti elektroninę informaciją gali tik Registro naudotojai, supažindinti su Registro saugos dokumentais ir pasirašę pasižadėjimus.

34. Už Registro naudotojų supažindinimą su Registro saugos dokumentais ir kitais saugos politikos įgyvendinamaisiais teisės aktais bei pasižadėjimų registravimą yra atsakingas Registro saugos įgaliotinis. Pakartotinai su Registro saugos dokumentais Registro naudotojai supažindinami tik iš esmės jiems pasikeitus.

35. Saugos nuostatai skelbiami Registro tvarkytojo interneto svetainėje.

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

_____