LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS
DĖL LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRO 2011 M. LIEPOS 1 D. ĮSAKYMO NR. V-659 „DĖL KRAUJO DONORŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO

2018 m. liepos 18 d. Nr. V-817
Vilnius

P a k e i č i u Lietuvos Respublikos sveikatos apsaugos ministro 2011 m. liepos 1 d. įsakymą Nr. V-659 „Dėl Kraujo donorų 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 ir 19 punktu, 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 Kraujo donorų 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. birželio 19 d. raštu Nr. (4.2) 6K-366

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos
ministro 2011 m. liepos 1 d.
įsakymu Nr. V-659
(Lietuvos Respublikos sveikatos apsaugos
ministro 2018 m. liepos 18 d.
įsakymo Nr. V-817
redakcija)

KRAUJO DONORŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kraujo donorų registro duomenų saugos nuostatai (toliau – saugos nuostatai) reglamentuoja Kraujo donorų registro (toliau – Registras) elektroninės informacijos saugos politiką ir kibernetinio saugumo politiką (toliau – elektroninės informacijos saugos politika), kurios tikslas – nustatyti ir įgyvendinti organizacines, technines ir kitas priemones, suteikiančias galimybę saugiai tvarkyti elektroninę informaciją ir užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo ar neteisėto tvarkymo.

2. 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 infrastruktūrai 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 infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“ (toliau – Kibernetinio saugumo reikalavimų aprašas), Kraujo donorų registro nuostatuose, patvirtintuose Lietuvos Respublikos sveikatos apsaugos ministro 1998 m. gruodžio 7 d. įsakymu Nr. 713 „Dėl Kraujo donorų 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 sveikatos apsaugos ministro tvirtinamus Registro saugos nuostatus ir saugos politiką įgyvendinančius dokumentus: saugaus elektroninės informacijos tvarkymo taisykles, naudotojų administravimo taisykles, veiklos tęstinumo valdymo planą (toliau visi kartu – saugos dokumentai).

5. Registro elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

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

5.2. Registre tvarkomų asmens duomenų apsauga;

5.3. Registro veikos tęstinumo užtikrinimas.

6. Saugos nuostatų reikalavimai taikomi:

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

6.2. Registro tvarkytojams:

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

6.2.2. kitiems Registro tvarkytojams – kraujo donorystės įstaigoms, licencijuotoms vykdyti kraujo donorystės veiklą (toliau – KDĮ);

6.3. Registro saugos įgaliotiniui;

6.4. Registro administratoriui;

6.5. Registro naudotojams;

6.6. paslaugų, susijusių su Registro veikimu, teikėjams.

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

8. Registro naudotojai ir paslaugų, susijusių su Registru, teikėjai 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 dokumentus, susijusius su elektroninės informacijos sauga;

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

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

9.4. atlieka kitas Valstybės informacinių išteklių valdymo įstatyme, Kibernetinio saugumo įstatyme, Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, Registro nuostatuose bei kituose teisės aktuose nustatytas funkcijas, susijusias su elektroninės informacijos sauga.

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

10.1. užtikrina ir atsako už Registro duomenų tvarkymo teisėtumą ir saugų Registro duomenų perdavimą kompiuterių tinklais (automatiniu būdu);

10.2. 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;

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

10.4. atlieka kitas Bendrųjų saugos reikalavimų aprašo, Kibernetinio saugumo reikalavimų aprašo, Registro saugos dokumentų bei kitų teisės aktų nustatytas funkcijas, susijusias su Registro elektroninės informacijos sauga.

11. Kitų Registro tvarkytojų funkcijos ir atsakomybė:

11.1. užtikrina Registro naudotojų laikymąsi Registro saugos politiką įgyvendinančiuose dokumentuose nurodytų reikalavimų bei darbo vietose naudojamų administracinių, techninių ir programinių priemonių, užtikrinančių elektroninės informacijos saugą, diegimo koordinavimą ir priežiūrą;

11.2. paskiria atsakingą asmenį atstovauti Registro tvarkytojui, bendradarbiaujant su pagrindiniu Registro tvarkytoju duomenų teikimo, tvarkymo, saugos reikalavimų laikymosi ir kitais organizaciniais ir techniniais klausimais;

11.3. atlieka kitas Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, Registro nuostatuose bei saugos dokumentuose nustatytas funkcijas.

12. Registro saugos įgaliotinio funkcijos ir atsakomybė:

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

12.2. teikia pagrindinio Registro tvarkytojo vadovui siūlymus dėl:

12.2.1. Registro administratoriaus paskyrimo;

12.2.2. Registro informacinių technologijų saugos atitikties vertinimo atlikimo;

12.3. teikia pasiūlymus Registro valdytojui dėl Registro saugos dokumentų priėmimo, keitimo arba naikinimo;

12.4. koordinuoja Registro saugos incidentų tyrimą;

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

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

12.7. turi teisę pagal savo įgaliojimus duoti privalomus vykdyti nurodymus ir pavedimus kitų Registro tvarkytojų darbuotojams, jeigu tai būtina saugos politikai įgyvendinti;

12.8. 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;

12.9. atlieka kitas Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, Registro saugos dokumentuose nustatytas funkcijas.

13. Registro administratoriaus funkcijos ir atsakomybė:

13.1. atsako už Registro techninės ir programinės įrangos funkcionavimą;

13.2. diegia ir prižiūri programinę įrangą, reikalingą pagrindinio Registro tvarkytojo funkcijoms vykdyti;

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

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

13.5. dalyvauja vykdant saugumo reikalavimų įgyvendinimo stebėseną;

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

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

13.8. atsako už Registro duomenų bazės atsarginių kopijų darymą;

13.9. atlieka kitas Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, Registro saugos dokumentuose nustatytas funkcijas.

14. Pagrindinio Registro tvarkytojo vadovo paskirtas kompetentingas asmuo, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą Higienos institute (toliau – kibernetinio saugumo vadovas), vykdo funkcijas, nustatytas Kibernetinio saugumo įstatyme, Kibernetinio saugumo reikalavimų apraše ir kituose kibernetinį saugumą reglamentuojančiuose teisės aktuose.

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

15.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

15.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

15.3. Lietuvos Respublikos kibernetinio saugumo įstatymas;

15.4. Bendrųjų saugos reikalavimų aprašas;

15.5. Kibernetinio saugumo reikalavimų aprašas;

15.6. 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“;

15.7. Registro nuostatai;

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

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

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

16. Registre tvarkoma elektroninė informacija priskiriama vidutinės svarbos informacijos kategorijai, vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo 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 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) 9.1 ir 9.2 papunkčių nuostatomis.

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

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

19. Registro saugos įgaliotinis, naudodamasis Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistema (toliau – ARSIS), kasmet atlieka Registro rizikos veiksnių vertinimą.

20. Registro grėsmių ir pažeidžiamumų, galinčių turėti įtakos informacinės sistemos kibernetiniam saugumui, vertinimas atliekamas kartu su Registro rizikos vertinimu. Registro rizikos vertinimo metu gali būti atliekamas pažeidžiamumų testavimas imituojant kibernetines atakas bei vykdant kibernetinių incidentų imitavimo pratybas.

21. Pagrindinės Registro rizikos mažinimo priemonės išdėstomos rizikos įvertinimo ataskaitoje, kurią kasmet iki gruodžio 31 d. rengia saugos įgaliotinis, įvertinęs galinčius turėti įtakos elektroninės informacijos saugai rizikos veiksnius, iš kurių svarbiausi yra šie:

21.1. 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);

21.2. 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);

21.3. 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.

22. Rizikos įvertinimo ataskaitos ir rizikos valdymo priemonių plano, jei toks buvo parengtas, duomenis bei jų kopijas pagrindinis 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“ (toliau – ARSIS nuostatai), nustatyta tvarka.

23. Elektroninės informacijos saugos būklė gerinama techninėmis, programinėmis ir organizacinėmis saugos priemonėmis, kurios pasirenkamos atsižvelgiant į Registro valdytojo skiriamus išteklius, vadovaujantis šiais principais:

23.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

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

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

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

25. 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.

26. Registro informacinių technologijų saugos reikalavimų atitikties vertinimui naudojama ARSIS.

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

28. Informacinių technologijų saugos atitikties vertinimo ataskaitas, pastebėtų trūkumų šalinimo plano duomenis ir jų kopijas pagrindinis Registro tvarkytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų patvirtinimo pateikia ARSIS nuostatų nustatyta tvarka.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

29. Programinės įrangos, skirtos Registrą apsaugoti nuo kenksmingosios programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos ir atnaujinimo reikalavimai:

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

29.2. programinė įranga turi automatiškai elektroniniu paštu informuoti Registro administratorių apie pagrindinio Registro tvarkytojo kompiuterizuotas darbo vietas ir tarnybines stotis, kuriose kenksmingosios programinės įrangos aptikimo priemonės netinkamai funkcionuoja, yra išjungtos arba neatsinaujino per 24 valandas;

29.3. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

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

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

30.2. Registro programinė įranga atnaujinama laikantis gamintojo reikalavimų;

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

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

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

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

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

32.2. visas duomenų srautas į internetą ir iš jo turi būti filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingosios programinės įrangos.

33. Leistinos kompiuterių naudojimo ribos:

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

33.2. nešiojamieji kompiuteriai Registro duomenims registruoti, kaupti ir naudoti gali būti naudojami tik KDĮ mobiliuosiuose punktuose, jais gali dirbti tik įgalioti asmenys;

33.3. nešiojamuosiuose kompiuteriuose turi būti naudojamas įjungimo slaptažodis, jie turi būti atskirti nuo viešojo interneto tinklo užkarda;

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

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

34.1. Registro elektroninė informacija perduodama per saugų valstybinį duomenų perdavimo tinklą (toliau – SVDPT) ir yra šifruojama;

34.2. Registro elektroninė informacija perduodama automatiniu būdu naudojant TCP/IP, HTTPS protokolus realiuoju laiku; iš susijusių registrų elektroninė informacija gaunama tik pagal duomenų teikimo sutartis, kuriose nustatytos perduodamos elektroninės informacijos specifikacijos, perdavimo sąlygos ir tvarka;

34.3. prieiga prie Registro suteikiama tik registruotiems Registro naudotojams;

34.4. tiesioginė prieiga prie Registro elektroninės informacijos suteikiama Registro naudotojui savo tapatybę patvirtinus slaptažodžiu. Registro naudotojų slaptažodžiai sudaromi, keičiami ir jų galiojimo trukmė nustatoma vadovaujantis Registro naudotojų administravimo taisyklėmis. Tiesioginė prieiga prie Registro užtikrinama ištisą parą darbo ir poilsio dienomis.

35. Pagrindinio Registro tvarkytojo naudotojų kompiuterizuotos darbo vietos turi būti valdomos naudojant centralizuoto valdymo priemones (pvz., katalogų tarnybą „*Active direktory*“).

36. Pagrindiniai atsarginių elektroninės informacijos kopijų darymo ir atkūrimo reikalavimai:

36.1. Registro elektroninės informacijos kopijos turi būti daromos automatiniu būdu kas 24 valandas; prireikus jas atkurti turi teisę Registro administratorius;

36.2. atsarginės elektroninės informacijos kopijos turi būti saugomos kitoje patalpoje nei Registro tarnybinės stotys.

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

37.1. 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;

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

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

39. 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 privalo laikytis Registro saugos dokumentuose nustatytų reikalavimų ir užtikrinti teikiamų paslaugų, vykdomų darbų ar tiekiamos įrangos atitiktį nustatytiems Kibernetinio saugumo reikalavimų aprašo reikalavimams.

40. 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.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

41. Registro saugos įgaliotinis ir kibernetinio saugumo vadovas privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, tobulinti kvalifikaciją elektroninės informacijos saugos srityje, savo darbe vadovautis Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą. Registro saugos įgaliotinis ar kibernetinio saugumo vadovas, pažeidęs Saugos nuostatų ar kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

42. 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.

43. 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, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

44. Administratorius ir Registro naudotojai turi būti susipažinę su Registro saugos dokumentais ir pagal kompetenciją su kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą.

45. Registro naudotojai raštu pasirašytinai įpareigojami saugoti asmens duomenų paslaptį. Įsipareigojimas saugoti asmens duomenų paslaptį galioja ir pasibaigus darbo santykiams, per visą asmens duomenų teisinės apsaugos laiką.

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

47. Registro saugos įgaliotinio, kibernetinio saugumo vadovo, Registro naudotojų ir Registro administratoriaus mokymų planavimo, organizavimo ir vykdymo tvarka:

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

47.2. Registro naudotojams turi būti įvairiais būdais primenama apie elektroninės informacijos saugos problemas (pvz., svarbios informacijos priminimai elektroniniu paštu, informacijos skelbimas Higienos instituto intranete, lankstinukai-atmintinės ir pan.);

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

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

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

V SKYRIUS
REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

48. Tvarkyti Registro duomenis ir gauti informaciją gali tik Registro naudotojai, susipažinę su saugos dokumentais, kuriais vadovaujamasi tvarkant elektroninę informaciją, ir raštu pasirašę pasižadėjimus saugoti asmens duomenų paslaptį. Pakartotinis supažindinimas su minėtais dokumentais vykdomas jiems pasikeitus.

49. Už Registro naudotojų supažindinimą su saugos dokumentais ir atsakomybe už šių reikalavimų nesilaikymą atsakingi Registro saugos įgaliotinis bei kitų Registro tvarkytojų vadovų paskirti atsakingi asmenys.

50. Saugos nuostatai skelbiami pagrindinio Registro tvarkytojo interneto svetainėje.

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

_____