Suvestinė redakcija nuo 2022-10-18

Įsakymas paskelbtas: Žin. 2009, Nr. 120-5167, i. k. 1092250ISAK000V-819

Nauja redakcija nuo 2014-12-18:
Nr. V-1264, 2014-12-03, paskelbta TAR 2014-12-17, i. k. 2014-19879

LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS DĖL MIRTIES ATVEJŲ IR JŲ PRIEŽASČIŲ VALSTYBĖS REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2009 m. rugsėjo 29 d. Nr. V-819
Vilnius

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, 9 punktu ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, 6 punktu:
Preambulės pakeitimai:
Nr. V-970, 2018-08-30, paskelbta TAR 2018-09-05, i. k. 2018-13994
Nr. V-1549, 2022-10-12, paskelbta TAR 2022-10-17, i. k. 2022-21017

1. T v i r t i n u Mirties atvejų ir jų priežasčių 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 Mirties atvejų ir jų priežasčių valstybės registro duomenų valdymo įgaliotinį, saugos įgaliotinį ir Registro administratorių;

2.2. pateikti Lietuvos Respublikos sveikatos apsaugos ministrui tvirtinti:

2.2.1. Mirties atvejų ir jų priežasčių valstybės registro naudotojų administravimo taisyklių projektą;

2.2.2. Mirties atvejų ir jų priežasčių valstybės registro saugaus elektroninės informacijos tvarkymo taisyklių projektą;

2.2.3. Mirties atvejų ir jų priežasčių valstybės registro veiklos tęstinumo valdymo plano projektą.

SVEIKATOS APSAUGOS MINISTRAS ALGIS ČAPLIKAS

PATVIRTINTA
Lietuvos Respublikos sveikatos
apsaugos ministro 2009 m. rugsėjo 29 d.
įsakymu Nr. V-819
(Lietuvos Respublikos sveikatos
apsaugos ministro 2022 m. spalio 12 d.
įsakymo Nr. V-1549
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 – saugos politika), organizacines, technines, programines, teisines ir kitas priemones, užtikrinančias saugų Registro elektroninės informacijos tvarkymą.

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 elektroninės informacijos saugos reikalavimų aprašas), Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – 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 Registro Saugos nuostatus ir saugos politiką įgyvendinančius dokumentus: Registro saugaus elektroninės informacijos tvarkymo taisykles, Registro naudotojų administravimo taisykles, Registro 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 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, LT-01506 Vilnius;

6.2. Registro tvarkytojui – Higienos institutui, Studentų g. 45A, LT-08107 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 valdytojo funkcijos:

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 teisės aktuose, reglamentuojančiuose valstybės registrų ir informacinių sistemų saugą, ir Registro nuostatuose nustatytas funkcijas.

10. Registro tvarkytojo funkcijos:

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. Registro valdytojo vadovo pavedimu skiria kibernetinio saugumo vadovą, Registro duomenų valdymo įgaliotinį, Registro saugos įgaliotinį ir Registro administratorių;

10.10. atlieka kitas Registro valdytojo pavestas bei teisės aktuose, reglamentuojančiuose valstybės registrų ir informacinių sistemų saugą, ir Registro nuostatuose nustatytas funkcijas.

11. Registro saugos įgaliotinio funkcijos ir atsakomybė:

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

11.2. organizuoja Registro informacinių technologijų saugos atitikties vertinimą ir parengia saugos atitikties vertinimo ataskaitą;

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

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

11.5. koordinuoja Registre įvykusių elektroninės informacijos saugos incidentų tyrimą;

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 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 Registro tvarkytojo vadovo pavestas 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 Registro tvarkytojo vadovo, Registro saugos įgaliotinio pavestas ir Registro saugos dokumentų jam priskirtas funkcijas.

13. Kibernetinio saugumo vadovas atlieka šias funkcijas:

13.1. koordinuoja kibernetinių incidentų tyrimą, bendradarbiauja su kompetentingomis institucijomis, tiriančiomis kibernetinius incidentus;

13.2. atlieka kitas Registro saugos dokumentuose nurodytas ir kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, jam priskirtas funkcijas.

14. Registro duomenų valdymo įgaliotinio funkcijos:

14.1. atlieka funkcijas, nustatytas Valstybės informacinių išteklių valdymo įstatymo 8 straipsnio 2 dalyje, ir kitas Registro saugos dokumentuose, kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą, nustatytas ir jam priskirtas funkcijas;

14.2. prireikus pagal kompetenciją teikia pasiūlymus Registro saugos įgaliotiniui dėl Saugos nuostatų 43 ir 44 punktuose nurodytų mokymų organizavimo Registro naudotojams elektroninės informacijos saugos ir kibernetinio saugumo klausimais.

15. Registro naudotojo funkcijos:

15.1. Registro saugos dokumentų nustatyta tvarka pagal kompetenciją tvarko Registro elektroninę informaciją, reikalingą jo funkcijoms atlikti;

15.2. pagal kompetenciją prireikus teikia pasiūlymus Registro saugos įgaliotiniui dėl Saugos nuostatų 43 ir 44 punktuose nurodytų mokymų organizavimo Registro naudotojams elektroninės informacijos saugos ir kibernetinio saugumo klausimais;

15.3. atlieka kitas Registro saugos dokumentuose, kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą, nustatytas ir jam priskirtas funkcijas.

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

16.1. Valstybės informacinių išteklių valdymo įstatymas;

16.2. 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);

16.3. Kibernetinio saugumo įstatymas;

16.4. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

16.5. 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);

16.6. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašas ir Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinti Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – Saugos atitikties vertinimo metodika);

16.7. Saugos dokumentų turinio 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“;

16.8. Kibernetinio saugumo reikalavimų aprašas;

16.9. Registro nuostatai;

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

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

17. Vadovaujantis Klasifikavimo gairių aprašo reikalavimais:

17.1. Registre tvarkoma elektroninė informacija pagal svarbą priskiriama vidutinės svarbos informacijos kategorijai;

17.2. pagal Registre tvarkomos elektroninės informacijos svarbą Registras priskiriamas trečios kategorijos informacinėms sistemoms.

18. Registro saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro prie Lietuvos Respublikos krašto apsaugos ministerijos (toliau – Kibernetinio saugumo centras) interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja Registro rizikos įvertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį Registro rizikos įvertinimą.

19. Registro rizikos vertinimo metu įvertinami rizikos veiksniai, galintys turėti įtakos Registro elektroninės informacijos saugai, jų galima žala, pasireiškimo tikimybė, rizikos laipsnis ir galimi rizikos valdymo būdai. Kartu su Registro rizikos vertinimu gali būti atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos Registro kibernetiniam saugumui, vertinimas. Svarbiausieji rizikos veiksniai nurodyti Bendrųjų elektroninės informacijos saugos reikalavimų apraše.

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

20.1. nereikšminga rizikos veiksnių tikimybė, žala – 1 balas;

20.2. maža rizikos veiksnių tikimybė, žala – 2 balai;

20.3. vidutinė rizikos veiksnių tikimybė, žala – 3 balai;

20.4. didelė rizikos veiksnių tikimybė, žala – 4 balai;

20.5. labai didelė rizikos veiksnių tikimybė, žala – 5 balai.

21. Registro rizikos įvertinimo rezultatai pateikiami rizikos įvertinimo ataskaitoje, kurią tvirtina Registro tvarkytojo vadovas. Prireikus tvirtinamas rizikos įvertinimo ir rizikos valdymo priemonių planas, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

22. Elektroninės informacijos saugos priemonių parinkimo principai:

22.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

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

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

22.4. parenkamos tokios saugos priemonės, kad būtų užtikrintas Registro veiklos tęstinumas ir saugus Registro darbas, patiriant kuo mažiau išlaidų.

23. Siekiant įvertinti saugos dokumentuose išdėstytų reikalavimų įgyvendinimo kontrolę, vadovaujantis Saugos atitikties vertinimo metodika, kartą per metus organizuojamas Registro informacinių technologijų saugos atitikties vertinimas.

24. Atlikus Registro informacinių technologijų saugos atitikties vertinimą, rengiama Registro informacinių technologijų saugos atitikties vertinimo ataskaita, prireikus – pastebėtų trūkumų šalinimo planas, kuriuos tvirtina Registro tvarkytojas.

25. Registro rizikos įvertinimo ataskaitos, rizikos valdymo priemonių plano, jei toks buvo rengtas, bei informacinių technologijų saugos atitikties vertinimo ataskaitos pastebėtų trūkumų šalinimo plano kopijas Registro tvarkytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų patvirtinimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai (toliau – ARSIS).

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 kenksmingosios programinės įrangos aptikimo priemonės, nuolat ieškančios ir blokuojančios kenksmingąją programinę įrangą ir atsinaujinančios automatiniu būdu;

26.2. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu;

26.3. elektroninės informacijos apsaugai naudojama programinė įranga turi turėti apsaugos mechanizmus, blokuojančius kenkimo programų bandymus panaikinti kenkimo programų apsaugas.

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 tinklai nuo viešųjų telekomunikacijų tinklų (interneto) turi būti atskirti ugniasienėmis, DoS (angl. *Denial of Service*) ir DDoS (angl.

Distributed Denial of Service) atakų prevencijai skirta įranga bei įsilaužimų aptikimo ir prevencijos įranga;

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

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. perduodama Registro elektroninė informacija yra šifruojama naudojant saugų SSL (angl. *Secure Sockets Layer*) protokolą;

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 registracijos slaptažodžių sistemą. Prieigos prie Registro elektroninės informacijos valdymas apibrėžtas Registro naudotojų administravimo taisyklėse.

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

32.1. atsarginės elektroninės informacijos kopijos (toliau – kopijos) turi būti daromos automatiniu būdu ne rečiau kaip kas 24 valandas;

32.2. kopijos turi būti saugomos kitoje patalpoje nei yra Registro tarnybinės stotys;

32.3. elektroninė informacija kopijose turi būti šifruojama;

32.4. kopijas turi teisę tvarkyti Registro administratorius arba techninės bei programinės įrangos priežiūros paslaugų teikėjai.

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

33.1. 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;

33.2. Kibernetinio saugumo centrui ir kitoms atsakingoms institucijoms pagal kompetenciją pranešama apie įvykusius saugos incidentus, jų vertinimą ir suvaldymą.

34. 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 asmuo, atliekantis Registro techninės ir programinės įrangos priežiūros ir duomenų, informacijos ir dokumentų ir (arba) jų kopijų tvarkymo funkcijas, negali turėti neišnykusio ar nepanaikinto teistumo už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat negali turėti paskirtos administracinės nuobaudos už Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 20 punkte nurodytus atvejus, jeigu nuo jos paskyrimo yra praėję mažiau kaip vieni metai, taip pat privalo laikytis Registro saugos dokumentuose nustatytų reikalavimų ir užtikrinti teikiamų paslaugų, vykdomų darbų ar tiekiamos įrangos atitiktį nustatytiems Kibernetinio saugumo reikalavimų aprašo reikalavimams.

35. 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

36. Registro saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis Lietuvos Respublikos teisės aktais ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą, tobulinti kvalifikaciją elektroninės informacijos saugos srityje.

37. Kibernetinio saugumo vadovas turi išmanyti kibernetinio saugumo užtikrinimo principus, tobulinti kvalifikaciją kibernetinio saugumo srityje ir savo darbe vadovautis Registro saugos dokumentais, Kibernetinio saugumo reikalavimų aprašu, Lietuvos Respublikos ir Europos Sąjungos teisės aktais, standartais, reglamentuojančiais kibernetinį saugumą.

38. Registro saugos įgaliotiniu 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 Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 20 punkte nurodytus atvejus, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai. Registro saugos įgaliotinis ir kibernetinio saugumo vadovas, pažeidęs Saugos nuostatų ar kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

39. Registro administratorius privalo išmanyti darbą su duomenų perdavimo tinklais, gebėti administruoti ir prižiūrėti Registro duomenų bazę.

40. Registro naudotojai privalo turėti darbo kompiuteriu įgūdžių, mokėti tvarkyti Registro duomenis Registro nuostatų nustatyta tvarka, būti susipažinę su Registro saugos dokumentais.

41. Registro naudotojai ir paslaugų, susijusių su Registru, teikėjai turi raštu pasirašytinai įsipareigoti saugoti asmens duomenų paslaptį. Įsipareigojimas saugoti asmens duomenų paslaptį galioja ir pasibaigus darbo santykiams, per visą asmens duomenų teisinės apsaugos laiką.

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

43. Kibernetinio saugumo vadovas arba Registro saugos įgaliotinis ne rečiau kaip kartą per dvejus metus inicijuoja Registro naudotojų mokymą elektroninės informacijos saugos ir kibernetinio saugumo klausimais, prireikus įvairiais būdais – pranešimais elektroniniu paštu, naujų darbuotojų instruktavimu, atmintinių rengimu, teminių seminarų organizavimu ir kitais informavimo būdais – primena apie saugumo problemas.

44. Registro naudotojų mokymai elektroninės informacijos saugos ir kibernetinio saugumo 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, Registro duomenų valdymo įgaliotinio ir Registro administratoriaus poreikius.

V SKYRIUS
REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

45. Tvarkyti Registro duomenis ir gauti informaciją gali tik Registro naudotojai, susipažinę su Registro saugos dokumentais, ir raštu pasirašę pasižadėjimus saugoti asmens duomenų paslaptį.

46. Už Registro naudotojų supažindinimą su Registro saugos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą atsakingas Registro saugos įgaliotinis. Pasikeitus Registro saugos dokumentams, Registro naudotojai su jais supažindinami pakartotinai.

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

Priedo pakeitimai:
Nr. V-970, 2018-08-30, paskelbta TAR 2018-09-05, i. k. 2018-13994
Nr. V-1549, 2022-10-12, paskelbta TAR 2022-10-17, i. k. 2022-21017

Pakeitimai:

1.
Lietuvos Respublikos sveikatos apsaugos ministerija, Įsakymas
Nr. V-1264, 2014-12-03, paskelbta TAR 2014-12-17, i. k. 2014-19879
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

2.
Lietuvos Respublikos sveikatos apsaugos ministerija, Įsakymas
Nr. V-970, 2018-08-30, paskelbta TAR 2018-09-05, i. k. 2018-13994
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

3.
Lietuvos Respublikos sveikatos apsaugos ministerija, Įsakymas
Nr. V-1549, 2022-10-12, paskelbta TAR 2022-10-17, i. k. 2022-21017
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