LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS
DĖL LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRO 2012 M. RUGSĖJO 28 D. ĮSAKYMO NR. V-920 „DĖL ŽMOGAUS AUDINIŲ, LĄSTELIŲ IR ORGANŲ DONORŲ BEI RECIPIENTŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO

2021 m. kovo 10 d. Nr. V-503
Vilnius

P a k e i č i u Lietuvos Respublikos sveikatos apsaugos ministro 2012 m. rugsėjo 28 d. įsakymą Nr. V-920 „Dėl Žmogaus audinių, ląstelių ir organų donorų bei recipientų 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 kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, 5 ir 6 punktais:“.

2. Pakeičiu nurodytu įsakymu patvirtintus Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro duomenų saugos nuostatus ir juos išdėstau nauja redakcija (pridedama).

Sveikatos apsaugos ministras Arūnas Dulkys

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2021 m. sausio 4 d. raštu Nr. (4.1 E) 6K-10

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro
2012 m. rugsėjo 28 d. įsakymu
Nr. V-920
(Lietuvos Respublikos sveikatos apsaugos
ministro 2021 m. kovo 10 d.
įsakymo Nr. V-503
redakcija)

ŽMOGAUS AUDINIŲ, LĄSTELIŲ IR ORGANŲ DONORŲ BEI RECIPIENTŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro (toliau – Registras) duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Registro elektroninės informacijos saugos ir kibernetinio saugumo valdymą, organizacinius ir techninius reikalavimus, reikalavimus personalui, dirbančiam su Registru, Registro naudotojų supažindinimo su saugos dokumentais principus.

2. Saugos nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2000 m. rugpjūčio 23 d. nutarimu Nr. 961 „Dėl Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro įsteigimo ir jo nuostatų patvirtinimo“ (toliau – Registro nuostatai), 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 – Saugos reikalavimai), Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Kibernetinio saugumo reikalavimų aprašas), Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų apraše ir Informacinių technologijų saugos atitikties vertinimo metodikoje, patvirtintuose 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 – Techniniai elektroninės informacijos saugos reikalavimai ir Informacinių technologijų saugos atitikties vertinimo metodika), ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą ir kibernetinio saugumo valdymą, vartojamas sąvokas.

3. Registro duomenų saugos tikslas – užtikrinti saugų Registro duomenų tvarkymą ir apdorojimą automatiniu būdu, vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (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) (toliau – BDAR), Saugos reikalavimais, Kibernetinio saugumo reikalavimų aprašu, kitais teisės aktais ir standartais, reglamentuojančiais saugų duomenų tvarkymą.

4. Registro duomenų saugumo užtikrinimo prioritetinės kryptys:

4.1. bendra fizinė informacijos apdorojimo priemonių (patalpų, kompiuterinės technikos ir vietinio tinklo, programinės įrangos naudotojų duomenų) apsauga;

4.2. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų Registro elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti, įgyvendinimas ir kontrolė;

4.3. Registro elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

4.4. Registre tvarkomų asmens duomenų apsauga.

5. Registro duomenų saugumo užtikrinimo prioritetiniai tikslai:

5.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti elektroninę informaciją;

5.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo ir nuo bet kokio neteisėto tvarkymo;

5.3. vykdyti elektroninės informacijos saugos incidentų, asmens duomenų saugumo pažeidimų prevenciją, reaguoti į elektroninės informacijos saugos incidentus, asmens duomenų saugumo pažeidimus ir juos operatyviai suvaldyti.

6. Saugos nuostatais turi vadovautis:

6.1. Lietuvos Respublikos sveikatos apsaugos ministerija – Registro valdytojas (Vilniaus g. 33, LT-01506, Vilnius);

6.2. Nacionalinis transplantacijos biuras prie Sveikatos apsaugos ministerijos – Registro tvarkytojas (Santariškių g. 2, LT-08661, Vilnius);

6.3. Registro saugos įgaliotinis (toliau – saugos įgaliotinis);

6.4. Registro administratorius;

6.5. duomenų valdymo įgaliotinis;

6.6. Registro duomenų naudotojai (toliau – Registro naudotojai).

7. Registro valdytojas vykdo šias funkcijas:

7.1. organizuoja Registro veiklą ir jai vadovauja, skiria arba paveda Registro tvarkytojui skirti saugos įgaliotinį ir duomenų valdymo įgaliotinį;

7.2. rengia ir tvirtina teisės aktus, susijusius su Registro tvarkymu ir duomenų sauga, bei prižiūri, kaip jų laikomasi;

7.3. priima sprendimą dėl Registro informacinių technologijų atitikties Saugos reikalavimams vertinimo atlikimo;

7.4. kontroliuoja, kad Registras būtų tvarkomas vadovaujantis Lietuvos Respublikos įstatymais, šiais Saugos nuostatais ir kitais teisės aktais;

7.5. nagrinėti Registro tvarkytojo pasiūlymus dėl Registro veiklos tobulinimo ir priima dėl jų sprendimus;

7.6. atlieka kitas teisės aktuose nustatytas funkcijas.

8. Registro tvarkytojas vykdo šias funkcijas:

8.1. Registro valdytojo pavedimu skiria saugos įgaliotinį ir paveda jam organizuoti ir kontroliuoti saugos dokumentų įgyvendinimą;

8.2. Registro valdytojo pavedimu skiria Registro administratorių ir paveda jam užtikrinti Registro serverio ir Registro naudotojų kompiuterizuotų darbo vietų saugų funkcionavimą, administruoti Registro duomenų bazę saugos dokumentų ir kitų teisės aktų nustatyta tvarka;

8.3. Registro valdytojo pavedimu skiria duomenų valdymo įgaliotinį;

8.4. atlieka Registro duomenų bazės techninę priežiūrą ir užtikrina nepertraukiamą Registro veiklą;

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

8.6. užtikrina, kad Registro naudotojai, turintys teisę naudotis Registro ištekliais numatytoms funkcijoms atlikti, laikytųsi reikalavimų, nustatytų Saugos nuostatuose bei kituose saugos politiką įgyvendinančiuose teisės aktuose;

8.7. teikia siūlymus Registro valdytojui dėl Registro sistemos veiklos tobulinimo, pagal kompetenciją atlieka Registro techninės, programinės įrangos priežiūros ir tobulinimo darbus;

8.8. atsako už Registro duomenų tvarkymo teisėtumą ir duomenų saugą bei Registro saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams ir šiems Saugos nuostatams;

8.9. atlieka kitas Registro nuostatuose, Saugos nuostatuose ir Registro saugos dokumentuose Registro valdytojo jam pavestas funkcijas.

9. Saugos įgaliotinis, įgyvendindamas Registro elektroninės informacijos saugą, atlieka šias funkcijas:

9.1. teikia Registro tvarkytojui pasiūlymus dėl:

9.1.1. Registro administratoriaus skyrimo;

9.1.2. saugos dokumentų priėmimo, keitimo ar panaikinimo;

9.1.3. saugos reikalavimų atitikties vertinimo atlikimo;

9.2. koordinuoja elektroninės informacijos saugos incidentų, įvykusių Registre, tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės;

9.3. teikia Registro administratoriui ir naudotojams privalomus vykdyti nurodymus bei pavedimus;

9.4. konsultuoja Registro naudotojus saugaus duomenų tvarkymo klausimais;

9.5. inicijuoja Registro naudotojų mokymą duomenų saugos klausimais, informuoja juos apie informacijos saugos problemas;

9.6. kasmet organizuoja Registro rizikos įvertinimą arba pagal poreikį organizuoja neeilinį Registro rizikos vertinimą;

9.7. atsako už duomenų saugumo politikos įgyvendinimą ir saugos dokumentų reikalavimų vykdymą;

9.8. informuoja Registro valdytoją ir kompetentingas institucijas apie neteisėtą veiklą, pažeidžiančią ar neišvengiamai pažeisiančią Registro saugą;

9.9. atlieka kitas saugos dokumentuose nurodytas ir šiais Saugos nuostatais jam priskirtas funkcijas.

10. Duomenų valdymo įgaliotinis:

10.1. įgyvendina Registro plėtrą;

10.2. tiesiogiai prižiūri, kaip kuriamas ir tvarkomas Registras, diegiama programinė įranga, panaudojamos investicijos;

10.3. rengia Registro biudžetų projektus;

10.4. teikia Registro tvarkytojui pasiūlymus dėl darbuotojų, kuriems pavesta tvarkyti duomenis, informaciją, dokumentus ir (arba) jų kopijas, teisių ir pareigų;

10.5. tiesiogiai prižiūri, kad informacija, duomenys, dokumentai ir (arba) jų kopijos būtų teikiami, skelbiami ir (arba) perduodami pagal teisės aktuose nustatytus reikalavimus;

10.6. atlieka kitas teisės aktuose nustatytas funkcijas.

11. Registro administratorius:

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

11.2. Registro naudotojams suteikia teisę naudotis duomenimis, reikalingais jiems priskirtoms funkcijoms atlikti;

11.3. administruoja Registro įrangą (kompiuterius, operacines sistemas, duomenų bazių valdymo sistemas, taikomųjų programų sistemas, ugniasienes, duomenų perdavimo tinklus ir kt.), nustato pažeidžiamas vietas ir saugos reikalavimų atitiktį;

11.4. įvertina, ar Registro naudotojai yra pasirengę darbui;

11.5. atsako už kompiuterių tinklo funkcionavimą;

11.6. atsako už Registro duomenų bazės atsarginių kopijų darymą ir archyve esančių kopijų saugojimą;

11.7. pagal kompetenciją dalyvauja vykdant saugumo reikalavimų įgyvendinimo stebėseną;

11.8. informuoja Registro saugos įgaliotinį apie saugos dokumentuose nustatytus reikalavimų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, elektroninės informacijos saugos incidentus;

11.9. teikia pasiūlymus dėl duomenų saugos organizavimo;

11.10. atsako už tai, kad tvarkant Registrą nebūtų pažeisti Saugos nuostatų reikalavimai;

11.11. atlieka kitas Registro tvarkytojo vadovo, saugos įgaliotinio pavestas ir Registro saugos dokumentuose jam nustatytas funkcijas.

12. Registro administratorius privalo patikrinti (peržiūrėti) Registro sąranką ir Registro būsenos rodiklius reguliariai, ne rečiau kaip kartą per metus ir (arba) po Registro pokyčio.

13. Tvarkant Registro duomenis ir užtikrinant jų saugą, vadovaujamasi šiais teisės aktais:

13.1. BDAR;

13.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

13.3. Lietuvos Respublikos kibernetinio saugumo įstatymu;

13.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

13.5. Saugos reikalavimais;

13.6. Kibernetinio saugumo reikalavimų aprašu;

13.7. Registro nuostatais;

13.8. Techniniais elektroninės informacijos saugos reikalavimais ir Informacinių technologijų saugos atitikties vertinimo metodika;

13.9. Nacionalinio kibernetinio saugumo centro prie Lietuvos Respublikos krašto apsaugos ministerijos interneto svetainėje skelbiama metodine priemone „Rizikos analizės vadovas“ (toliau – Rizikos analizės vadovas), Lietuvos standartais LST EN ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, LST EN ISO/IEC 27002:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“, taip pat kitais Lietuvos ir tarptautiniais grupės „Informacijos technologija. Saugumo technika“ standartais, reglamentuojančiais saugų duomenų tvarkymą;

13.10. Saugos nuostatais ir kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugumo politiką ir Registro duomenų tvarkymo teisėtumą bei duomenų saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

14. 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 – Elektroninės informacijos svarbos nustatymo gairių aprašas), 9.1 ir 9.2 papunkčiais, Registro tvarkoma informacija priskiriama prie vidutinės svarbos informacijos kategorijos.

15. Vadovaujantis Elektroninės informacijos svarbos nustatymo gairių aprašo 12.3 papunkčiu, Registras priskiriamas prie trečiosios kategorijos informacinių sistemų – Registre tvarkoma vidutinės svarbos informacija.

16. Registro elektroninės informacijos sauga šiuose Saugos nuostatuose suprantama kaip administracinių, techninių ir programinių priemonių, skirtų duomenų konfidencialumui (kad su Registre tvarkoma informacija galėtų susipažinti tik tam įgalioti asmenys), vientisumui (kad duomenys nebūtų atsitiktinai ar neteisėtai pakeisti ar sunaikinti) ir prieinamumui (kad duomenys galėtų būti tvarkomi reikiamu metu) užtikrinti, visuma.

17. Saugos įgaliotinis, atsižvelgdamas į Rizikos analizės vadovą, Lietuvos ir tarptautinius grupės „Informacijos technologija. Saugumo technika“ standartus, kasmet organizuoja Registro rizikos įvertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį rizikos įvertinimą.

18. Vertinant riziką turi būti:

18.1. nustatomos grėsmės ir pažeidžiamumai, galintys paveikti Registro elektroninės informacijos saugą;

18.2. nustatomos galimos grėsmių ir pažeidžiamumo poveikio sritys vykdomai veiklai;

18.3. įvertinama Registro pažeidimo grėsmių tikimybė ir pasekmės;

18.4. nustatomas rizikos lygis, įvertinamos nustatytos grėsmių tikimybės, kurios išdėstomos prioriteto tvarka pagal svarbą, nustatomą atsižvelgiant į atliktą rizikos vertinimą.

19. 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, galintys pažeisti Registro duomenų ir parengtos pagal juos informacijos saugą, yra:

19.1. subjektyvūs netyčiniai (duomenų tvarkymo klaidos ir apsirikimai, duomenų ištrynimas, klaidingas duomenų teikimas, fiziniai informacijos technologijų sutrikimai, duomenų perdavimo tinklais sutrikimai, programinės įrangos klaidos, netinkamas veikimas ir kita);

19.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis Registro duomenims gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugos pažeidimai, vagystės ir kita);

19.3. atsitiktinės subjektyvios aplinkybės (darbuotojų praradimas, vandens poveikis, elektros instaliacijos gedimas ir kita);

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

21. Registro valdytojas, atsižvelgdamas į Registro rizikos įvertinimo ataskaitą, prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

22. Rizikos veiksnių tikimybės Registro duomenų bazės duomenų konfidencialumo, vientisumo, prieinamumo pažeidimo rizikos vertinimo klasifikacija yra:

22.1. labai maža rizika – 1 balas;

22.2. maža rizika – 2 balai;

22.3. vidutinė rizika – 3 balai;

22.4. didelė rizika – 4 balai;

22.5. labai didelė rizika – 5 balai.

23. 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.

24. Parenkamos tokios saugos priemonės, kad būtų užtikrintas Registro veiklos tęstinumas, patiriant kuo mažiau išlaidų ir užtikrinant saugų Registro darbą.

25. Saugos įgaliotinis, Registro valdytojo arba jo pavedimu Registro tvarkytojo vidaus auditorius ar kitas Registro valdytojo arba jo pavedimu Registro tvarkytojo paskirtas vertintojas (toliau – vertintojas), siekdamas užtikrinti Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose išdėstytų nuostatų įgyvendinimą ir saugumo politikos laikymosi kontrolę, ne rečiau kaip kartą per metus organizuoja Registro informacinių technologijų saugos reikalavimų atitikties vertinimą.

26. Registro informacinių technologijų saugos reikalavimų atitikties vertinimo metu:

26.1. įvertinama, ar reali duomenų saugos situacija atitinka Saugos nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų reikalavimus;

26.2. inventorizuojama Registro techninė ir programinė įranga;

26.3. tikrinamos Registro tvarkymo kompiuterizuotos darbo vietos ir registre įdiegtos programos bei jų sąranka (konfigūracija);

26.4. patikrinama Registro naudotojams suteiktų teisių tvarkyti Registrą ir jų vykdomų funkcijų atitiktis;

26.5. tikrinamas pasirengimas atkurti Registro veiklą elektroninės informacijos saugos (kibernetinio) incidento atveju;

26.6. tikrinamas įdiegtos antivirusinės ir apsaugos nuo nepageidaujamos programinės įrangos filtravimo sistemų naudojimas, valdymas, atnaujinimas;

26.7. tikrinamas programinės įrangos, programinės įrangos sertifikatų ir licencijų naudojimas;

26.8. tikrinamas tarnybinių stočių ir komunikacinės įrangos naudojimas;

26.9. tikrinama, kaip daromos duomenų bazių atsarginės kopijos ir archyvai;

26.10. vertinami kiti Informacinių technologijų saugos atitikties vertinimo metodikos 5 punkte nurodyti kriterijai.

27. Atlikus Registro informacinių technologijų saugos reikalavimų atitikties vertinimą, vertintojas, vadovaudamasis Informacinių technologijų saugos atitikties vertinimo metodikos 4 punktu, pateikia informacinių technologijų saugos reikalavimų įgyvendinimo lygio vertinimą nuo vieneto iki penketo ir parengia pastebėtų trūkumų šalinimo planą, jeigu tokie nustatomi, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato Registro valdytojas.

28. Registro rizikos įvertinimo ataskaitos, Registro rizikos įvertinimo ir rizikos valdymo priemonių plano, Registro informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas Registro valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 10 d. įsakymu Nr. V-1183, nustatyta tvarka.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

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

29.1. teisė dirbti su konkrečia elektronine informacija suteikiama konkrečiam Registro naudotojui arba Registro naudotojų grupei;

29.2. nutrūkus tarnybiniams santykiams ar pasibaigus darbo sutarčiai, Registro naudotojo teisė naudotis Registru turi būti panaikinta. Registro naudotojo teisė dirbti su konkrečia elektronine informacija turi būti ribojama ar sustabdoma, kai vyksta Registro naudotojo veiklos tyrimas, naudotojas yra ilgalaikėse atostogose arba perkeliamas į kitas pareigas ir keičiasi pareigybės aprašyme nurodytos ar atliekamos funkcijos;

29.3. Registro naudotojas turi imtis priemonių, kad su Registro duomenimis negalėtų susipažinti pašaliniai asmenys;

29.4. prisijungimo prie kompiuterių tinklo laikas ir trukmė nėra ribojami, Registro informacinė sistema pasiekiama visą parą;

29.5. prisijungimo ryšiai koduojami SSL kodavimo priemonėmis ar kitomis lygiavertėmis kodavimo priemonėmis;

29.6. duomenys turi būti šifruojami patikimu SSL („VeriSign“ arba lygiaverčiu) sertifikatu, patikrinamu PGP raktu ar kitomis lygiavertėmis šifravimo priemonėmis.

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

30.1. tarnybinėse stotyse ir kompiuterizuotose darbo vietose turi būti naudojamos centralizuotai valdomos kenksmingosios programinės įrangos aptikimo priemonės, kurios turi būti reguliariai atnaujinamos automatiniu būdu;

30.2. šios priemonės turi nuolat ieškoti ir blokuoti kenksmingąsias programas, veikiančias sisteminiuose kataloguose esančiose rinkmenose (įskaitant suspaustas rinkmenas) serveryje ir visuose kompiuterių tinklo kompiuteriuose;

30.3. turi turėti apsaugos mechanizmus, blokuojančius kenksmingųjų programų bandymus panaikinti apsaugas nuo kenkimo programų;

30.4. apsaugai naudojama programinė įranga privalo atsinaujinti ne rečiau kaip kartą per 24 valandas.

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

31.1. Registro funkcijoms vykdyti leidžiama naudoti tik legalią programinę įrangą;

31.2. programinė įranga turi būti nuolatos atnaujinama, laikantis gamintojų reikalavimų;

31.3. draudžiama naudoti programinę įrangą, nesusijusią su įstaigos veikla;

31.4. turi būti naudojama Registro administravimo programinės įrangos ugniasienė;

31.5. turi būti įdiegta galimybė nustatyti asmenis, kurie naudojosi prieiga prie Registro duomenų, fiksuoti jų atliktus veiksmus ir juos kaupti;

31.6. turi būti sudaryta galimybė visas užklausas Registro duomenų bazei fiksuoti programiniu būdu;

31.7. Registro naudotojų prieiga prie Registro duomenų leidžiama tik per registravimosi ir slaptažodžių sistemą. Registro administratorius savo tapatybę turi patvirtinti slaptažodžiu, kuriam keliami aukštesni reikalavimai negu Registro naudotojų slaptažodžiams;

31.8. turi būti įgyvendinta prievolė ne rečiau kaip kas tris mėnesius keisti slaptažodžius;

31.9. Registro naudotojų prieigos valdymas apibrėžtas Registro naudotojų administravimo taisyklėse;

31.10. programinės įrangos naudotojo instrukcijos (vadovai), duomenų tvarkymo taisyklės ir duomenų saugos reikalavimai naudotojams visuomet prieinami.

32. Leistinos kompiuterių naudojimo ribos:

32.1. stacionarūs 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 informacija;

32.2. kompiuterinė įranga ir duomenų perdavimo tinklo mazgai turi turėti atsarginį maitinimo šaltinį, užtikrinantį šios įrangos veikimą ne trumpiau kaip 30 minučių;

32.3. nešiojamieji kompiuteriai prie Registro kompiuterių tinklo gali būti prijungiami ir iš Registro tvarkymo patalpų išnešami tik saugos įgaliotiniui leidus;

32.4. kiekvienas stacionarus kompiuteris priskiriamas atsakingam Registro naudotojui;

32.5. stacionarų kompiuterį įjungti (išjungti iš) Registro kompiuterių tinklo gali tik Registro administratorius;

32.6. stacionarūs kompiuteriai gali būti išnešami ir įnešami tik Registro administratoriui leidus;

32.7. Registro naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo. Duomenys, susiję su Registru, nešiojamuose kompiuteriuose turi būti šifruojami arba turi būti įdiegtos kitos techninės priemonės, kurios užtikrintų šių duomenų apsaugą.

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

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

33.2. 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*) bei kitų per tinklą vykdomų atakos rūšių;

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

34. Viešaisiais telekomunikaciniais tinklais perduodamos elektroninės informacijos konfidencialumas užtikrinamas naudojant saugų valstybinį duomenų perdavimo tinklą.

35. Registro duomenys iš susijusių registrų gaunami automatiniu būdu pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas.

36. Registro fizinę saugą užtikrina šios saugos priemonės: gaisro ir įsilaužimo jutikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų, kontroliuojamas patekimas į darbo vietas ir kita.

37. Registrui administruoti naudojamas operacines sistemas, techninę ir programinę įrangą, reikalingą Registro naudotojo funkcijoms vykdyti, diegia ir prižiūri tik Registro administratorius.

38. Registro programinę įrangą diegti ar atnaujinti turi tik Registro administratorius ar įgalioti asmenys.

39. Registro programinė įranga turi būti testuojama naudojant atskirą tam skirtą testavimo aplinką.

40. Prarasti, iškraipyti, sunaikinti Registro duomenys atkuriami iš Registro atsarginių duomenų kopijų. Registro atsarginių duomenų kopijos daromos automatiniu būdu kiekvieną darbo dieną esant aktyviai Registro duomenų bazei. Kopijos įrašomos į keičiamus informacijos kaupiklius (kompaktinius diskus ar magnetines juostas) ir saugomos seife, prieinamame tik Registro administratoriui, jo nesant – Registro administratorių pavaduojančiam asmeniui. Jas atkurti turi teisę tik Registro administratorius ar jį pavaduojantis asmuo. Kopijų, iš kurių būtų galima atkurti registro duomenis, darymo ir saugojimo tvarka išsamiai aprašyta Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro saugaus elektroninės informacijos tvarkymo taisyklėse, patvirtintose Lietuvos Respublikos sveikatos ministro 2013 m. sausio 21 d. įsakymu Nr. V-70 „Dėl Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro saugaus elektroninės informacijos tvarkymo taisyklių, Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro veiklos tęstinumo plano ir Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro naudotojų administravimo taisyklių patvirtinimo“.

41. Registrui keliami organizaciniai ir techniniai kibernetinio saugumo reikalavimai įgyvendinami vadovaujantis Kibernetinio saugumo reikalavimų aprašu.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

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

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

44. Registro administratoriumi gali būti skiriamas asmuo, išmanantis darbą su kompiuterių tinklais ir mokantis užtikrinti jų saugumą. Registro administratorius turi būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais, Registro nuostatais, Saugos nuostatais, Registro saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą.

45. Duomenų valdymo įgaliotinis yra Registro tvarkytojo vadovas arba jo paskirtas darbuotojas, atsakingas už Registro tvarkytojo teisės aktuose nustatytų funkcijų atlikimą.

46. Registro naudotojai privalo turėti pagrindinius darbo kompiuteriu įgūdžius, mokėti tvarkyti Registro elektroninę informaciją Registro nuostatų nustatyta tvarka, būti susipažinę su Saugos nuostatais bei teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą.

47. Registro naudotojai, pastebėję, kad yra saugos dokumentų pažeidimų, nusikalstamos veikos požymių, kad neveikia arba netinkamai veikia duomenų saugos užtikrinimo priemonės, privalo nedelsdami apie tai pranešti Registro administratoriui arba saugos įgaliotiniui.

48. Saugos įgaliotinis periodiškai inicijuoja Registro naudotojų mokymą informacijos saugos klausimais, įvairiais būdais (priminimai elektroniniu paštu, teminių seminarų rengimas ir (ar) organizavimas, atmintinės priimtiems naujiems darbuotojams ir panašiai) informuoja juos apie informacijos saugos (kibernetinio saugumo) problemas.

49. Registro naudotojams ir Registro administratoriui mokymus gali vykdyti saugos įgaliotinis ar kitas Registro valdytojo ar Registro tvarkytojo darbuotojas, išmanantis elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus arba elektroninės informacijos saugos (kibernetinio saugumo) mokymų paslaugų teikėjas.

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

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

50.2. mokymai Registro naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per dvejus metus. Mokymai saugos įgaliotiniui, Registro administratoriui turi būti organizuojami pagal poreikį.

51. Registro saugos dokumentai iš esmės turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per kalendorinius metus. Saugos dokumentai taip pat turi būti persvarstomi (peržiūrimi) atlikus rizikos veiksnių analizę ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams.

52. Įvykus elektroninės informacijos saugos incidentui, saugos įgaliotinio, Registro administratoriaus ir Registro naudotojų veiksmus reglamentuoja Registro veiklos tęstinumo valdymo planas.

V SKYRIUS
REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

53. Tvarkyti Registro duomenis gali tik įgalioti Registro naudotojai, susipažinę su saugos dokumentais ir raštu sutikę laikytis saugos dokumentuose nustatytų reikalavimų.

54. Registro naudotojų supažindinimą su saugos dokumentais ir atsakomybe už saugos dokumentuose nustatytų reikalavimų nesilaikymą pasirašytinai organizuoja saugos įgaliotinis. Saugos įgaliotinis raštu informuoja Registro naudotojus apie saugos dokumentų priėmimą, pakeitimą ar pripažinimą netekusiais galios.

55. Pakartotinai su Registro saugos dokumentais Registro naudotojai supažindinami jiems pasikeitus.

56. Saugos nuostatai bei kiti dokumentai, reglamentuojantys saugų elektroninės informacijos tvarkymą, skelbiami Registro tvarkytojo Dokumentų valdymo sistemoje arba (ir) Registro tvarkytojo internetinėje svetainėje.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

57. Saugos įgaliotinis, Registro administratorius ir Registro naudotojai, pažeidę šių Saugos nuostatų ir kitų saugų informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako teisės aktų nustatyta tvarka.

58. Įsigyjant viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugas, elektroninės informacijos prieglobos paslaugas, skaitmenines paslaugas, jų teikėjams taikomi reikalavimai, nustatyti Kibernetinio saugumo reikalavimų apraše.

_____