Suvestinė redakcija nuo 2014-11-08 iki 2018-07-24

Įsakymas paskelbtas: Žin. 2011, Nr. 82-4020, i. k. 1112250ISAK000V-659

Nauja redakcija nuo 2014-11-08:
Nr. V-1145, 2014-11-05, paskelbta TAR 2014-11-07, i. k. 2014-16277

LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS DĖL KRAUJO DONORŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2011 m. liepos 1 d. Nr. V-659
Vilnius

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

1. T v i r t i n u Kraujo donorų 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 Kraujo donorų registro duomenų valdymo įgaliotinį, saugos įgaliotinį ir administratorių;

2.2. pateikti Lietuvos Respublikos sveikatos apsaugos ministrui tvirtinti:

2.2.1. Kraujo donorų registro naudotojų administravimo taisyklių projektą;

2.2.2. Kraujo donorų registro saugaus elektroninės informacijos tvarkymo taisyklių projektą;

2.2.3. Kraujo donorų registro veiklos tęstinumo valdymo plano projektą.

SVEIKATOS APSAUGOS MINISTRAS RAIMONDAS ŠUKYS

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos
ministro 2011 m. liepos 1 d.
įsakymu Nr. V-659
(Lietuvos Respublikos sveikatos apsaugos
ministro 2014 m. lapkričio 5 d.
įsakymo Nr. V-1145 redakcija)

KRAUJO DONORŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kraujo donorų registro (toliau – Registras) duomenų saugos nuostatai (toliau – saugos nuostatai) reglamentuoja Registro elektroninės informacijos saugos valdymą, organizacinius ir techninius reikalavimus, reikalavimus personalui.

2. Registro saugos nuostatuose vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, Kraujo donorų registro nuostatuose, patvirtintuose Lietuvos Respublikos sveikatos apsaugos ministro 1998 m. gruodžio 7 d. įsakymu Nr. 713 „Dėl Kraujo donorų registro nuostatų patvirtinimo ir veiklos pradžios nustatymo“ (toliau – Registro nuostatai), kituose teisės aktuose ir Lietuvos Respublikos standartuose LST ISO/IEC 27002:2009 ir LST ISO/IEC 27001:2006.

3. Registro elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

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

3.2. prieigos prie Registro elektroninės informacijos kontrolė;

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

3.4. Registro duomenų konfidencialumo užtikrinimas.

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

5. Saugos nuostatų reikalavimai taikomi:

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

5.2. Registro tvarkytojams:

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

5.2.2. kitoms Registro tvarkytojoms – kraujo donorystės įstaigoms, licencijuotoms vykdyti kraujo donorystės veiklą (toliau – KDĮ);

5.3. Registro saugos įgaliotiniui;

5.4. Registro administratoriui;

5.5. Registro naudotojams.

6. Registro valdytojo funkcijos ir atsakomybė:

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

6.2. tvirtina Registro saugos nuostatus, saugaus elektroninės informacijos tvarkymo taisykles, veiklos tęstinumo valdymo planą, naudotojų administravimo taisykles (toliau visi kartu – saugos dokumentai) ir kitus teisės aktus, kuriuose reglamentuojama saugi ir teisėta Registro tvarkymo tvarka ir nustatomi Registro elektroninės informacijos saugos reikalavimai;

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

6.4. skiria arba paveda pagrindiniam Registro tvarkytojui skirti Registro duomenų valdymo įgaliotinį, Registro saugos įgaliotinį ir Registro administratorių;

6.5. vykdo kitas Registro nuostatais, saugos dokumentais ir kitais saugos politiką įgyvendinančiais teisės aktais jam priskirtas funkcijas.

7. Pagrindinio Registro tvarkytojo funkcijos ir atsakomybė:

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

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

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

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

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

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

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

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

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

7.10. vykdo kitas Registro valdytojo pavestas, Registro nuostatais, saugos dokumentais ir kitais saugos politiką įgyvendinančiais teisės aktais jam priskirtas funkcijas.

8. Kitų Registro tvarkytojų funkcijos ir atsakomybė:

8.1. vykdo saugos nuostatų 7.1–7.3 ir 7.10 papunkčiuose nurodytas funkcijas;

8.2. užtikrina, kad jų įstaigose dirbantys Registro naudotojai laikytųsi Registro saugos dokumentuose ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą, nurodytų reikalavimų;

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

9. Registro saugos įgaliotinio funkcijos ir atsakomybė:

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

9.2. teikia pagrindinio Registro tvarkytojo vadovui siūlymus dėl:

9.2.1. Registro administratoriaus paskyrimo ir reikalavimų administratoriui nustatymo;

9.2.2. Registro saugos atitikties vertinimo atlikimo;

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

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

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

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

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

9.8. 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;

9.9. atlieka kitas pagrindinio Registro tvarkytojo vadovo pavestas, Registro saugos nuostatais ir kitais saugos politiką įgyvendinančiais dokumentais jam priskirtas funkcijas.

10. Registro administratoriaus funkcijos ir atsakomybė:

10.1. atsako už Registro techninės ir programinės įrangos funkcionavimą;

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

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

10.4. 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;

10.5. dalyvauja vykdant saugumo reikalavimų įgyvendinimo stebėseną;

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

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

10.8. atsako už Registro duomenų bazės atsarginių kopijų darymą;

10.9. atlieka kitas pagrindinio Registro tvarkytojo vadovo, saugos įgaliotinio pavestas, Registro saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose jam priskirtas funkcijas.

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

11.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

11.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

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

11.4. 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“;

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

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

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

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

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

12. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 4 ir 5 punktais:

12.1. Registre tvarkoma elektroninė informacija pagal svarbą priskiriama žinybinės svarbos elektroninės informacijos kategorijai. Priskyrimo šiai kategorijai kriterijai: Registro elektroninės informacijos praradimas gali padaryti žalą vieno ar kelių fizinių ar juridinių asmenų teisėtiems interesams ir asmens duomenų apsaugai, taip pat gali turėti neigiamų padarinių institucijos veiklai;

12.2. Registras priskiriamas trečios kategorijos informacinėms sistemoms, priskyrimo šiai kategorijai kriterijus – Registre apdorojama žinybinės svarbos informacija.

13. Vadovaujantis Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms 7 punktu, Registre automatiniu būdu tvarkomi asmens duomenys priskiriami trečiam asmens duomenų saugumo lygiui.

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

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

15.1. 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, neteisingas veikimas ir kita);

15.2. 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);

15.3. 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.

16. Registro rizikos veiksniams vertinti naudojama penkiabalė rizikos veiksnio tikimybės ir poveikio vertinimo sistema, pagal kurią apskaičiuojamas rizikos laipsnis:

16.1. rizikos laipsnis nuo 1 iki 6 balų – maža rizika;

16.2. rizikos laipsnis nuo 8 iki 12 balų – vidutinė rizika;

16.3. rizikos laipsnis nuo 15 iki 25 balų – didelė rizika.

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

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

19. Elektroninės informacijos saugos priemonių parinkimo principai:

19.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

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

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

20. Siekiant įvertinti Registro saugos dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, kartą per dvejus metus organizuojamas Registro saugos atitikties vertinimas.

21. Atlikus Registro saugos atitikties vertinimą, rengiama Registro saugos atitikties vertinimo ataskaita, kuri pateikiama pagrindinio Registro tvarkytojo vadovui.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

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

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

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

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

23. Programinės įrangos, įdiegtos tarnybinėse stotyse ir pagrindinio Registro tvarkytojo kompiuteriuose, naudojimo nuostatos:

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

23.2. programinė įranga turi būti nuolat atnaujinama laikantis gamintojo reikalavimų;

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

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

24. Pagrindinio Registro tvarkytojo kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kita) pagrindinės naudojimo nuostatos:

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

24.2. 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);

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

25. Leistinos kompiuterių naudojimo ribos:

25.1. 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;

25.2. nešiojamieji kompiuteriai Registro duomenims registruoti, kaupti ir naudoti gali būti naudojami tik KDĮ mobiliuosiuose punktuose;

25.3. mobiliuosiuose punktuose nešiojamaisiais kompiuteriais gali dirbti tik tam įgalioti asmenys;

25.4. nešiojamieji kompiuteriai turi būti atskirti nuo viešojo interneto tinklo užkarda;

25.5. nešiojamuosiuose kompiuteriuose turi būti naudojamas įjungimo slaptažodis;

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

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

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

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

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

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

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

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

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

27. Registro veiklos tęstinumui ir funkcionalumui užtikrinti elektroninė informacija automatiniu būdu kopijuojama kas 24 valandas. Kartą per savaitę daromos atsarginės

elektroninės informacijos kopijos, kurios turi būti saugomos kitoje patalpoje nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

28. Saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, tobulinti kvalifikaciją elektroninės informacijos saugos srityje, savo darbe vadovautis Registro saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų duomenų tvarkymą, privalo prižiūrėti, kaip įgyvendinama saugos politika.

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

30. 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.

31. Registro naudotojai privalo turėti darbo kompiuteriu įgūdžių, mokėti tvarkyti Registro duomenis Registro nuostatų nustatyta tvarka, būti susipažinę su Registro saugos dokumentais ir pasirašę pasižadėjimus saugoti konfidencialią informaciją apie asmens duomenis (toliau – pasižadėjimai).

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

V SKYRIUS
REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

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

34. Už Registro naudotojų supažindinimą su Registro saugos nuostatais ir kitais saugos politiką įgyvendinančiais dokumentais bei pasižadėjimų registravimą yra atsakingas Registro saugos įgaliotinis. Pakartotinai su Registro saugos dokumentais Registro naudotojai supažindinami tik iš esmės jiems pasikeitus.

35. Registro saugos įgaliotinis saugos dokumentus pateikia kitų Registro tvarkytojų vadovų paskirtiems atsakingiems asmenims, kurie su jais supažindina savo įstaigoje dirbančius Registro naudotojus ir atsako už jų pasirašytų pasižadėjimų perdavimą Registro saugos įgaliotiniui.

36. Saugos nuostatai skelbiami pagrindinio Registro tvarkytojo interneto svetainėje.

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

_____

Priedo pakeitimai:
Nr. V-1145, 2014-11-05, paskelbta TAR 2014-11-07, i. k. 2014-16277

Pakeitimai:

1.
Lietuvos Respublikos sveikatos apsaugos ministerija, Įsakymas
Nr. V-1145, 2014-11-05, paskelbta TAR 2014-11-07, i. k. 2014-16277
Dėl Lietuvos Respublikos sveikatos apsaugos ministro 2011 m. liepos 1 d. įsakymo Nr. V-659 "Dėl Kraujo donorų registro duomenų saugos nuostatų patvirtinimo" pakeitimo