PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro
2013 m. sausio 21 d. įsakymu Nr. V-70
(Lietuvos Respublikos sveikatos apsaugos ministro
2021 m. balandžio 22 d. įsakymo Nr. V-892
redakcija)

# ŽMOGAUS AUDINIŲ, LĄSTELIŲ IR ORGANŲ DONORŲ BEI RECIPIENTŲ REGISTRO SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

## I SKYRIUS
## BENDROSIOS NUOSTATOS

1. Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) nustato saugų Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro (toliau – Registras) elektroninės informacijos tvarkymą ir kibernetinio saugumo užtikrinimą.

2. Taisyklės parengtos vadovaujantis šiais teisės aktais:

2.1. Saugos dokumentų turinio gairių aprašu, patvirtintu 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“;

2.2. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau - Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas);

2.3. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašu ir Informacinių technologijų saugos atitikties vertinimo metodika, patvirtintais 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“;

2.4. Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro nuostatais, patvirtintais 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) ir kitais Registro saugos dokumentais;

2.5. kitais teisės aktais, reglamentuojančiais duomenų tvarkymą.

3. Taisyklėse vartojamos sąvokos atitinka teisės aktuose, kuriais vadovaujantis parengtos šios Taisyklės, ir kituose saugų elektroninės informacijos bei duomenų tvarkymą reglamentuojančiuose teisės aktuose apibrėžtas sąvokas.

4. Elektroninės informacijos savybės:

4.1. konfidencialumas – su Registre tvarkoma elektronine informacija gali susipažinti tik tam įgalioti asmenys;

4.2. vientisumas – elektroninė informacija nebuvo atsitiktiniu ar neteisėtu būdu pakeista ar sunaikinta;

4.3. prieinamumas – elektroninė informacija gali būti tvarkoma reikiamu metu.

5. Registre saugomi ir apdorojami Žmogaus audinių, ląstelių ir organų donorų bei recipientų duomenys.

6. Registre esanti elektroninė informacija skirstoma į kategorijas:

6.1. duomenys apie asmenis, pareiškusius sutikimą (nesutikimą), kad jų audiniai ir (ar) organai po jų mirties būtų panaudoti transplantacijai;

6.2. duomenys apie gyvus donorus;

6.3. duomenys apie mirusius donorus;

6.4. duomenys apie recipientus;

6.5. duomenys ir informacija apie audinių, ląstelių, organų paėmimą, transplantaciją ir šalinimą;

6.6. Registro objekto registravimo Registre duomenys ir informacija;

6.7. duomenų ir informacijos įrašymo bei keitimo datos;

6.8. duomenų teikėjo, pateikusio duomenis ir informaciją, duomenys;

6.9. už duomenų ir informacijos teisingumą atsakingo asmens identifikavimo duomenys – vardas, pavardė.

7. Registre tvarkomos elektroninės informacijos sąrašas yra pateiktas Registro nuostatų skyriuje „Registro duomenys ir informacija“.

8. 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.

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

10. Taisyklės privalomos Registro valdytojui, Registro tvarkytojui, Registro naudotojams, Registro administratoriui bei saugos įgaliotiniui. Už Registro tvarkymo taisyklių įgyvendinimo organizavimą ir kontrolę atsako Registro saugos įgaliotinis.

11. Už Registro elektroninės informacijos tvarkymą atsakingi:

11.1. Registro administratorius – už duomenų, nurodytų Registro nuostatų 15 punkte tvarkymą, už Registro administravimą, duomenų bazių atkūrimą ir priežiūrą, prieinamumo užtikrinimą, klasifikatorių tvarkymą;

11.2. registruoti Registro naudotojai.

## II SKYRIUS
## TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

12. Registro kompiuterinės įrangos saugos priemonės:

12.1. siekiant užtikrinti Registro patikimumą bei jame saugomų ir apdorojamų duomenų konfidencialumą, vientisumą ir prieinamumą, turi būti įdiegti duomenų bazių bei rinkmenų tarnybinių stočių klasteriai, viena kitą dubliuojančios užkardos, keli interneto prieigos serveriai, dubliuoti tinklo komutatoriai, patikima duomenų saugykla ir rezervinio kopijavimo įranga;

12.2. visa Registro kompiuterių aparatinė įranga privalo turėti šios įrangos gamintojų garantinį arba pratęstą pogarantinį aptarnavimą;

12.3. Registro kompiuterių aparatinė įranga gali būti keičiama tik gavus Nacionalinio transplantacijos biuro prie Sveikatos apsaugos ministerijos (toliau – Biuras) direktoriaus leidimą;

12.4. visi Registro kompiuterių aparatinės įrangos gedimai ir keitimai turi būti registruojami žurnale. Už gedimų registravimą atsakingas Registro administratorius;

12.5. Registro programinė sistema turi perspėti Registro administratorius, kai tarnybinėse stotyse sumažėja iki nustatytos pavojingos ribos laisvos operatyviosios atminties ar vietos diske

(diskuose) ar duomenų saugykloje, ilgą laiką stipriai apkraunamas centrinis procesorius ar tinklo sąsaja;

12.6. Registro techninės ir programinės įrangos priežiūrą ir gedimų šalinimą atlieka kvalifikuoti specialistai.

13. Registro sisteminės ir taikomosios programinės įrangos saugos priemonės:

13.1. Registre gali būti naudojama tik legali, Registro funkcijoms vykdyti būtina sisteminė ir taikomoji programinė įranga. Programinę įrangą gali diegti tik Registro administratorius arba paslaugų teikėjas;

13.2. sisteminės ir taikomosios programinės įrangos apsaugai nuo virusų ir kitų kenkėjiškų programų Registre turi būti naudojama specializuota, nuolat automatiškai atnaujinama programinė įranga;

13.3. Registro programinė įranga prižiūrima laikantis gamintojo rekomendacijų;

13.4. Registro tarnybinių stočių įvykių žurnaluose turi būti registruojami ir ne mažiau kaip 1 (vienus) metus saugomi duomenys (nurodant įvykio laiką ir Registro naudotojo identifikatorių) apie Registro įjungimą ir išjungimą, sėkmingus ir nesėkmingus bandymus registruotis Registre, bandymus prieiti prie Registro informacinių išteklių, kitus Registro saugomų ir apdorojamų duomenų saugai svarbius įvykius. Registro tarnybinių stočių įvykių žurnalai turi būti analizuojami ne rečiau kaip kartą per dvi savaites;

13.5. kiekvienas Registro naudotojas ir Registro administratorius turi būti unikaliai identifikuojamas, todėl visiems Registro naudotojams ir Registro administratoriams, vadovaujantis Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro naudotojų administravimo taisyklėmis, patvirtintomis Lietuvos Respublikos sveikatos apsaugos 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 valdymo plano ir Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro naudotojų administravimo taisyklių patvirtinimo“, suteikiamas Registro naudotojo ar Registro administratoriaus vardas bei nustatomi Registro naudotojo ar Registro administratoriaus tapatybę patvirtinančių slaptažodžių reikalavimai;

13.6. Registro priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą Registro administratoriaus identifikatorių, kuriuo naudojantis nebūtų galima atlikti Registro naudotojo funkcijų;

13.7. slaptažodžiai, suteikiantys teisę administruoti Registrą ir Registro naudotojus, žinomi tik Registro administratoriui. Tam, kad nesant Registro administratoriaus Registrą galėtų administruoti jį pavaduojantis asmuo, Registro administratorių slaptažodžiai saugomi Biuro direktoriaus seife. Perėmus Registro administravimą pagrindiniam Registro administratoriui, Registro administratoriaus slaptažodį privaloma pakeisti nauju;

13.8. Registro naudotojo teisė dirbti su konkrečia elektronine informacija turi būti ribojama ar sustabdoma, kai Registro naudotojas atostogauja, vykdomas jo veiklos tyrimas ir pan.;

13.9. Registro naudotojo teisė naudotis Registro duomenimis turi būti panaikinta pasibaigus tarnybos (darbo) santykiams;

13.10. Registro naudotojui baigus darbą turi būti imamasi priemonių, kad su Registre saugomais duomenimis negalėtų susipažinti pašaliniai asmenys:

13.11. atsijungiama nuo Registro;

13.12. įjungiama ekrano užsklanda su slaptažodžiu;

13.13. dokumentai ir laikmenos padedami į pašaliniams asmenims neprieinamą vietą ir pan.;

13.14. Registro naudotojui neatliekant jokių veiksmų, Registras turi taip užsirakinti, kad toliau juo naudotis galima būtų tik pakartojus tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus;

13.15. Registro sisteminės ir taikomosios programinės įrangos keitimas ir atnaujinimas gali būti atliekami gavus Biuro direktoriaus leidimą;

13.16. visi Registro kompiuterių sisteminės ir taikomosios programinės įrangos keitimai bei atnaujinimai turi būti registruojami žurnale.

14. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

14.1. siekiant užtikrinti elektroninės informacijos konfidencialumą ir vientisumą, šios informacijos teikimas bei priėmimas turi būti vykdomas naudojant Saugų valstybinį duomenų perdavimo tinklą arba kitą saugų šifruotą duomenų perdavimo kanalą;

14.2. Registro tarnybinės stotys, Registro tvarkytojo naudotojų kompiuterizuotos darbo vietos ir kita kompiuterinė įranga, įjungta į elektroninės informacijos perdavimo tinklą, yra atskirta nuo viešųjų ryšių tinklų naudojant ugniasienes, ugniasienių įvykių žurnalai reguliariai analizuojami;

14.3. Registro programinė įranga apsaugota nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XXS (angl. *Cross-site scripting*), atkirtimo nuo paslaugų (angl. *DOS*), dedikuoto atkirtimo nuo paslaugos (angl. *DDOS*);

14.4. Registro tinklo perimetro apsaugai naudojami filtrai, apsaugantys viešame ryšių tinkle naršančių Registro naudotojų kompiuterinę įrangą nuo kenksmingo kodo;

14.5. nuotolinis prisijungimas viešaisiais ryšių tinklais prie Registro leidžiamas tik iš nustatytų IP adresų;

14.6. viešai prieinama Registro elektroninė informacija turi būti saugoma atskirame kompiuterių potinklyje – vadinamojoje demilitarizuotoje zonoje.

15. Patalpų ir aplinkos saugumo užtikrinimo priemonės:

15.1. patalpos atitinka priešgaisrinės saugos reikalavimus, jose yra gaisro gesinimo priemonių ir periodiškai vykdoma gaisro gesinimo patikra;

15.2. patalpos atskirtos nuo bendrojo naudojimo patalpų, asmenys, nesusiję su Registro tvarkymu, patekti į šias patalpas gali tik lydimi Registro administratoriaus;

15.3. veikia patekimo į patalpas kontrolės sistema;

15.4. techninė įranga įnešama ir išnešama iš patalpų tik Registro saugos įgaliotiniui leidus;

15.5. ryšių kabeliai apsaugoti nuo pažeidimo ir neteisėto prisijungimo prie jų;

15.6. įgyvendintos gamintojo nustatytos techninės įrangos darbo sąlygos;

15.7. patalpų durys šarvuotos ir apsaugotos dviem skirtingos konstrukcijos spynomis;

15.8. patalpose įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų;

15.9. į patalpą, kurioje saugomi serveriai, gali patekti tik tie asmenys, kuriems tai būtina atliekant darbo funkcijas ar Biurui teikiant paslaugas su Biuro direktoriaus leidimu;

15.10. patalpose naudojami nepertraukiamo elektros maitinimo šaltiniai.

16. Kitos priemonės, naudojamos elektroninės informacijos saugai užtikrinti:

16.1. Registro duomenų bazės veiksmų žurnale fiksuojami elektroninės informacijos pakeitimą atlikusio Registro naudotojo duomenys ir pakeitimo laikas;

16.2. kiekvienas naudotojas, prieš naudodamasis Registru, savo tapatybę patvirtina slaptažodžiu;

16.3. kiekvienam naudotojui Registre suteikiamos tik tiesioginėms pareigoms vykdyti būtinos teisės;

16.4. Registro naudotojų darbo vietose naudojamos tik tarnybinėms reikmėms skirtos išorinės duomenų laikmenos (USB, CD/DVD ir kt.);

16.5. išorinėje duomenų laikmenoje teikiami asmens duomenys ir sveikatos asmens duomenys šifruojami arba naudojamos kitos saugos priemonės, užtikrinančios, kad asmens duomenys ir sveikatos asmens duomenys bus perduoti saugiai ir nebus galimybės tretiesiems asmenims jais pasinaudoti;

16.6. išoriniais duomenų perdavimo tinklais perduodami asmens duomenys ir sveikatos asmens duomenys šifruojami;

16.7. per metus turi būti užtikrintas Registro prieinamumas ne mažiau kaip 90 proc. laiko darbo metu darbo dienomis.

## III SKYRIUS
## SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

17. Saugaus elektroninės informacijos keitimo, atnaujinimo, įvedimo ir naikinimo užtikrinimo tvarka:

17.1. Registro elektroninės informacijos keitimą, atnaujinimą, įvedimą ir naikinimą gali atlikti tik tokią teisę turintys autorizuoti Registro naudotojai;

17.2. administravimo posistemyje tvarkomus duomenis įvesti, keisti, atnaujinti ar naikinti turi teisę tik Registro administratorius;

17.3. Registre saugomi ir apdorojami duomenys įvedami, atnaujinami, keičiami ir naikinami Registro nuostatuose nustatyta tvarka.

18. Registro naudotojų veiksmų registravimo tvarka: siekiant nustatyti neteisėtus veiksmus su Registre saugomais ir apdorojamais duomenimis bei šių duomenų vientisumo pažeidimus, Registro naudotojų veiksmai, jų darbo su Registru laikas turi būti automatiškai registruojami elektroniniuose žurnaluose.

19. Registro naudotojų ir Registro administratoriaus atliekamų veiksmų auditui turi būti registruojama ši informacija:

19.1. Registro elementų įjungimas ir išjungimas ar perkrovimas;

19.2. Registro naudotojų, administratoriaus prisijungimas (ir nesėkmingi bandymai prisijungti) ir atsijungimas;

19.3. audito funkcijos įjungimas ir išjungimas;

19.4. audito įrašų trynimas, kūrimas ar keitimas.

20. Kiekviename audito duomenų įraše turi būti fiksuojama įvykio data ir tikslus laikas, įvykio rūšis ir pobūdis, Registro naudotojo, Registro administratoriaus ir (arba) Registro įrenginio, susijusio su įvykiu, duomenys, įvykio rezultatas. Audito duomenų įrašai saugomi 30 dienų. Draudžiama audito duomenis trinti, keisti, kol nesibaigęs audito duomenų saugojimo terminas.

21. Registro atsarginių elektroninės informacijos kopijų darymo saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarka:

21.1. Registro duomenų kopijos automatiniu būdu daromos kartą per parą ir įrašomos į išorinę duomenų laikmeną;

21.2. informacija apie elektroninės informacijos kopijavimą (kopijos įrašymo data ir laikas) automatiškai fiksuojama ir saugoma Registro tarnybinės stoties veiksmų žurnale;

21.3. prarasti, iškraipyti ar sunaikinti Registro duomenys turi būti atkuriami iš Registro duomenų atsarginių kopijų. Registro neveikimo laikotarpis negali būti ilgesnis nei 16 val.;

21.4. Registro elektroninė informacija atsarginėse kopijose yra šifruojama;

21.5. už Registro duomenų atkūrimą iš atsarginių duomenų kopijų atsakingas Registro administratorius.

22. Saugaus elektroninės informacijos perkėlimo ir teikimo susijusioms informacinėms sistemoms, elektroninės informacijos gavimo iš jų užtikrinimo tvarka:

22.1. Registro duomenys kitiems registrams teikiami ir gaunami iš jų su šių registrų valdytojais sudarytose duomenų teikimo sutartyse numatytais būdais, apimtimi, reguliarumu ir terminais;

22.2. Registro duomenys kitiems registrams perduodami laikantis Registro nuostatuose, Registro saugos politiką įgyvendinančiuose dokumentuose nurodytų reikalavimų;

22.3. duomenų teikėjai duomenis Registrui teikia Registro nuostatų nustatyta tvarka;

22.4. už duomenų, gaunamų iš susijusių registrų ir kitų informacinių sistemų, atnaujinimo procesą Registre yra atsakingas Registro administratorius.

23. Elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo (toliau – neteisėta veikla) nustatymas:

23.1. Registro administratorius privalo naudoti visas įmanomas aparatines, programines ir administracines priemones, skirtas apsisaugoti nuo neteisėtos veiklos;

23.2. siekiant patikrinti, ar su Registro duomenimis nėra vykdoma neteisėta veikla, Registro administratorius kiekvieną darbo dieną privalo peržiūrėti Registro programinės įrangos elektroniniuose žurnaluose sukauptus atitinkamus įrašus;

23.3. kilus įtarimui, kad su Registru ir jame saugomais ir apdorojamais duomenimis yra vykdoma neteisėta veikla, Registro administratorius nedelsdamas privalo apie tai informuoti Registro saugos įgaliotinį;

23.4. Registro saugos įgaliotinis, gavęs pranešimą apie neteisėtą veiklą, inicijuoja saugos incidentų valdymo procedūros vykdymą;

23.5. Registro naudotojas, pastebėjęs neteisėtos veiklos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdamas pranešti apie tai Registro administratoriui.

24. Registro programinės ir techninės įrangos keitimo ir atnaujinimo (toliau – pokyčiai) tvarka:

24.1. visi pokyčiai (projektavimas, kūrimas, testavimas, diegimas) atliekami Registro tvarkytojo ir (ar) Registro valdytojo iniciatyva;

24.2. pokyčių projektavimą ir kūrimą atlieka Registro tvarkytojo vadovo paskirti atsakingi darbuotojai arba įstatymų nustatyta tvarka pasirinkti paslaugų teikėjai tam skirtoje kūrimo aplinkoje. Atsakomybė už pokyčių įgyvendinimo sprendimus nustatoma pokyčių projektavimo ir kūrimo dokumentacijoje;

24.3. prieš atliekant keitimus, kurių metu gali iškilti grėsmė Registro elektroninės informacijos konfidencialumui, vientisumui ar pasiekiamumui, visi pakeitimai turi būti išbandomi testavimo aplinkoje;

24.4. įgyvendinant pokyčius, kurių metu galimi Registro veikimo sutrikimai, Registro administratorius privalo ne vėliau kaip prieš vieną darbo dieną iki planuojamų pokyčių vykdymo pradžios informuoti (elektroniniu paštu, faksu ar kitomis priemonėmis) Registro naudotojus apie tokių darbų pradžią ir galimus sutrikimus;

24.5. atlikęs pokyčių testavimą arba jei testavimo darbų dėl programinių ir (ar) techninių priežasčių nebuvo galima atlikti, Registro administratorius gali pradėti įgyvendinti pokyčius;

24.6. jeigu testavimas sėkmingas, pokyčiai perkeliami į gamybinę aplinką;

24.7. visi pokyčiai registruojami ir prireikus apie tai informuojami Registro naudotojai;

24.8. Registro administratorius Registro naudotojams privalo pateikti visą reikalingą informaciją apie naudojimosi Registru pakitimus, kurie yra susiję su jų atliekamomis funkcijomis ir kurių atsiradimas susijęs su įvykdytais arba vykdomais pokyčiais.

25. Nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių naudojimo tvarka:

25.1. Nešiojamaisiais kompiuteriais turi teisę naudotis tik Registro naudotojai ir Registro administratorius darbinėms funkcijoms atlikti;

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

25.3. nešiojamuosiuose kompiuteriuose turi būti naudojamas kompiuterio slaptažodis;

25.4. baigus darbą ar pasitraukiant iš darbo vietos, Registro naudotojai privalo imtis priemonių, kad su Registro duomenimis negalėtų susipažinti pašaliniai asmenys (atsijungti nuo Registro, įjungti ekrano užsklandą su slaptažodžiu);

25.5. Registro elektroninė informacija nešiojamuosiuose kompiuteriuose turi būti šifruojama;

25.6. nešiojamieji kompiuteriai, nedirbant su jais, turi būti saugomi saugioje vietoje.

## IV SKYRIUS
## REIKALAVIMAI, KELIAMI INFORMACINIŲ SISTEMŲ FUNKCIONAVIMUI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

26. Registro priežiūros paslaugų tiekėjams suteikiami tokie prieigos prie Registro lygiai ir sąlygos, kurie reikalingi ir pakankami priežiūros paslaugoms pagal nustatytus reikalavimus atlikti.

27. Perkant paslaugas, darbus ar įrangą, susijusius su Registru, pirkimo dokumentuose turi būti iš anksto nustatyta, kad paslaugos teikėjas turi užtikrinti atitiktį kibernetinio saugumo reikalavimams, nustatytiems Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše.

## V SKYRIUS
## BAIGIAMOSIOS NUOSTATOS

28. Asmenys, pažeidę šių Taisyklių reikalavimus, atsako teisės aktų nustatyta tvarka.

_____