***Suvestinė redakcija nuo 2016-01-06 iki 2018-01-18***

*Įsakymas paskelbtas: Žin. 2012, Nr. 82-4316, i. k. 11223IRISAK0005V-57*

***Nauja redakcija nuo 2015-09-25:***
*Nr. 5V-49, 2015-09-24, paskelbta TAR 2015-09-24, i. k. 2015-14176*

# INFORMATIKOS IR RYŠIŲ DEPARTAMENTO PRIE LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS DIREKTORIUS

# ĮSAKYMAS DĖL ĮTARIAMŲJŲ, KALTINAMŲJŲ IR NUTEISTŲJŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2012 m. liepos 4 d. Nr. 5V-57
Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 43 straipsnio 2 dalimi ir 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 7.1 papunkčiu ir 8 punktu:

1. T v i r t i n u Įtariamųjų, kaltinamųjų ir nuteistųjų registro duomenų saugos nuostatus (pridedama).

2. S k i r i u Įtariamųjų, kaltinamųjų ir nuteistųjų registro saugos įgaliotiniu Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos Saugos skyriaus vyriausiąją specialistę Aistę Raudoniūtę.

*Punkto pakeitimai:*
*Nr. 5V-1, 2016-01-05, paskelbta TAR 2016-01-05, i. k. 2016-00079*

3. P a v e d u Įtariamųjų, kaltinamųjų ir nuteistųjų registro saugos įgaliotiniui per 5 mėnesius nuo šio įsakymo įsigaliojimo dienos teisės aktų nustatyta tvarka parengti ir pateikti Informatikos ir ryšių departamento direktoriui tvirtinti saugos politiką įgyvendinančius dokumentus – Įtariamųjų, kaltinamųjų ir nuteistųjų registro veiklos tęstinumo valdymo planą ir Įtariamųjų, kaltinamųjų ir nuteistųjų registro saugaus duomenų tvarkymo taisykles.

4. N u s t a t a u, kad Įtariamųjų, kaltinamųjų ir nuteistųjų registro naudotojai administruojami vadovaujantis Vidaus reikalų informacinės sistemos centrinio duomenų banko naudotojų administravimo taisyklėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2008 m. rugpjūčio 18 d. įsakymu Nr. 1V-165.

DIREKTORIUS GINTARAS ČIURLIONIS

PATVIRTINTA
Informatikos ir ryšių departamento
prie Lietuvos Respublikos vidaus
reikalų ministerijos direktoriaus
2012 m. liepos 4 d. įsakymu
Nr. 5V-57
(Informatikos ir ryšių
departamento prie Lietuvos
Respublikos vidaus reikalų
ministerijos direktoriaus
2015 m. rugsėjo 24 d. įsakymo
Nr. 5V-49 redakcija)

# ĮTARIAMŲJŲ, KALTINAMŲJŲ IR NUTEISTŲJŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

## I. BENDROSIOS NUOSTATOS

1. Įtariamųjų, kaltinamųjų ir nuteistųjų registro duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Įtariamųjų, kaltinamųjų ir nuteistųjų registro (toliau – Registras) duomenų saugos politiką, kurios tikslas – nustatyti ir įgyvendinti organizacines, technines ir kitas priemones, suteikiančias galimybę saugiai tvarkyti Registro duomenis, Registro informaciją, Registrui pateiktus dokumentus ir (arba) jų kopijas (toliau – Registro duomenys) ir užtikrinti, kad Registro duomenys būtų patikimi ir apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo ar neteisėto jų tvarkymo.

2. Saugos nuostatuose vartojamos sąvokos:

2.1. Registro saugos politiką įgyvendinantys dokumentai – Registro valdytojo patvirtinti dokumentai: Registro saugaus duomenų tvarkymo taisyklės ir Registro veiklos tęstinumo valdymo planas bei Vidaus reikalų informacinės sistemos centrinio duomenų banko naudotojų administravimo taisyklės, patvirtintos Lietuvos Respublikos vidaus reikalų ministro 2008 m. rugpjūčio 18 d. įsakymu Nr. 1V-165 „Dėl Vidaus reikalų informacinės sistemos centrinio duomenų banko naudotojų administravimo taisyklių patvirtinimo“ (toliau – VRIS CDB naudotojų administravimo taisyklės);

2.2. kitos Saugos nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme (toliau – Valstybės informacinių išteklių valdymo įstatymas), 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“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas), Įtariamųjų, kaltinamųjų ir nuteistųjų

registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2012 m. balandžio 18 d. nutarimu Nr. 435 „Dėl Įtariamųjų, kaltinamųjų ir nuteistųjų registro nuostatų patvirtinimo ir veiklos pradžios nustatymo“ (toliau – Registro nuostatai) vartojamas sąvokas.

3. Registro saugos tikslas – užtikrinti Registro duomenų konfidencialumą, prieinamumą ir vientisumą ir sudaryti sąlygas saugiai automatiniu būdu tvarkyti Registro duomenis.

4. Registro duomenų saugos užtikrinimo prioritetinės kryptys:

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

4.2. Registro veiklos tęstinumo užtikrinimas;

4.3. Registre tvarkomų asmens duomenų apsauga.

5. Registro duomenų saugai užtikrinti kompleksiškai naudojamos administracinės, techninės ir programinės priemonės.

6. Saugos nuostatai taikomi:

6.1. Registro valdytojui – Informatikos ir ryšių departamentui prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Informatikos ir ryšių departamentas) (Šventaragio g. 2, Vilnius);

6.2. Registro tvarkytojams:

6.2.1. Informatikos ir ryšių departamentui;

6.2.2. Lietuvos Respublikos Prezidento kanceliarijai (S. Daukanto a. 3, Vilnius), ikiteisminio tyrimo įstaigoms ir bausmių vykdymo institucijoms – laisvės atėmimo vietoms ir probacijos tarnyboms (toliau – kiti Registro tvarkytojai).

7. Registro valdytojo funkcijos ir atsakomybė:

7.1. rengia ir priima teisės aktus, susijusius su Registro duomenų tvarkymu ir sauga, kontroliuoja, kaip jų laikomasi;

7.2. priima sprendimus dėl Registrui taikomų informacinių technologijų saugos atitikties vertinimo atlikimo;

7.3. atsižvelgdamas į informacinių technologijų saugos atitikties vertinimo ataskaitą, prireikus tvirtina trūkumų šalinimo planą;

7.4. užtikrina Registro funkcijų pokyčių valdymo planavimą;

7.5. atsako už Registro saugos politikos formavimą, jos įgyvendinimo organizavimą, priežiūrą;

7.6. atlieka kitas Saugos nuostatų, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Registro nuostatų ir kitų teisės aktų nustatytas funkcijas, susijusias su Registro duomenų sauga.

8. Informatikos ir ryšių departamento, kaip Registro tvarkytojo, funkcijos ir atsakomybė:

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

8.2. atlieka kitas Saugos nuostatų, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Registro nuostatų ir kitų teisės aktų nustatytas funkcijas, susijusias su Registro duomenų sauga.

9. Kitų Registro tvarkytojų funkcijos ir atsakomybė:

9.1. atsako už tvarkomų pagal kompetenciją Registro duomenų saugą;

9.2. teikia pasiūlymus Registro valdytojui, kaip tobulinti Registro duomenų saugą;

9.3. užtikrina tinkamą Registro valdytojo priimtų teisės aktų ir rekomendacijų, susijusių su Registro duomenų sauga, tinkamą įgyvendinimą;

9.4. atlieka kitas Saugos nuostatų, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Registro nuostatų ir kitų teisės aktų nustatytas funkcijas, susijusias su Registro duomenų sauga.

10. Registro saugos įgaliotinio (toliau – Saugos įgaliotinis) funkcijos ir atsakomybė:

10.1. teikia Registro valdytojo vadovui pasiūlymus dėl:

10.1.1. Registro administratoriaus paskyrimo ir reikalavimų Registro administratoriui nustatymo;

10.1.2. Registro informacinių technologijų saugos atitikties vertinimo atlikimo Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 43 punkte nurodytoje metodikoje nustatyta tvarka;

10.1.3. Registro saugos dokumentų priėmimo, keitimo ar panaikinimo;

10.2. koordinuoja Registro saugos incidentų tyrimą;

10.3. teikia Registro administratoriui ir Registro naudotojams privalomus vykdyti nurodymus ir pavedimus dėl Registro saugos politikos įgyvendinimo;

10.4. organizuoja Registro saugos rizikos vertinimą;

10.5. periodiškai organizuoja Registro naudotojų mokymą Registro duomenų saugos klausimais, įvairiais būdais informuoja juos apie Registro duomenų saugos problemas;

10.6. įgyvendindamas Registro duomenų saugą, yra atsakingas už tinkamą Saugos nuostatuose nustatytų funkcijų vykdymą;

10.7. atlieka kitas Registro valdytojo vadovo pavestas, Saugos nuostatų, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir kitų teisės aktų nustatytas funkcijas.

11. Administratorius, vykdantis Registro priežiūrą, atlieka šias funkcijas:

11.1. pagal kompetenciją užtikrina Registro duomenų konfidencialumą, vientisumą ir prieinamumą;

11.2. registruoja Registro saugos incidentus ir informuoja apie juos Saugos įgaliotinį, teikia Registro valdytojui pasiūlymus dėl minėtų incidentų pašalinimo;

11.3. suteikia, keičia ir panaikina Registro naudotojams prieigos prie Registro duomenų teises;

11.4. rengia, tikrina ir atnaujina Registro komponentų techninę sąranką ir jos būsenos rodiklius;

11.5. vykdo Saugos įgaliotinio nurodymus ir pavedimus, susijusius su Registro saugos užtikrinimu;

11.6. atlieka kitas Registro valdytojo vadovo pavestas, Saugos reikalavimų, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir kitų teisės aktų nustatytas funkcijas;

11.7. atlikdamas Registro funkcijų pakeitimus, Registro administratorius turi vadovautis Vidaus reikalų informacinės sistemos pokyčių valdymo tvarkos aprašu, patvirtintu Lietuvos Respublikos vidaus reikalų ministro 2007 m. gruodžio 29 d. įsakymu Nr. 1V-453 „Dėl Vidaus reikalų informacinės sistemos pokyčių valdymo tvarkos aprašo patvirtinimo“;

11.8. vykdydamas Registro priežiūrą, yra atsakingas už tinkamą Saugos nuostatuose nustatytų funkcijų vykdymą.

12. Teisės aktai, kuriais vadovaujantis tvarkomi Registro duomenys ir užtikrinama jų sauga:

12.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

12.2. Valstybės informacinių išteklių valdymo įstatymas;

12.3. Lietuvos Respublikos kibernetinio saugumo įstatymas;

12.4. Lietuvos Respublikos Įtariamųjų, kaltinamųjų ir nuteistųjų registro įstatymas;

12.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

12.6. Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ (toliau – Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas);

12.7. 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“;

12.8. Bendrieji reikalavimai organizacinėms ir techninėms asmens 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 asmens duomenų saugumo priemonėms patvirtinimo“ (toliau – Bendrieji reikalavimai organizacinėms ir techninėms asmens duomenų saugumo priemonėms);

12.9. Registro nuostatai;

12.10. aktualūs Lietuvos standartai LST ISO/IEC 27002 ir LST ISO/IEC 27001 bei Lietuvos ir tarptautiniai „Informacijos technologijos. Saugumo metodai“ grupės standartai, reglamentuojantys saugų duomenų tvarkymą;

12.11. kiti teisės aktai, reglamentuojantys Registro duomenų tvarkymo teisėtumą, Registro valdytojo ir Registro tvarkytojų veiklą ir Registro duomenų saugos valdymą.

## II. REGISTRO ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

13. Atsižvelgiant į galimo Registro duomenų savybių (vientisumo, konfidencialumo ir prieinamumo) praradimo pasekmes, Registre tvarkomi duomenys priskirtini ypatingos svarbos elektroninės informacijos kategorijai vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 4.1.2, 4.1.7 ir 4.2.7 papunkčių nuostatomis.

14. Registras priskiriamas pirmajai kategorijai vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 5.1 papunkčio nuostatomis, atsižvelgiant į valstybės registre apdorojamos elektroninės informacijos svarbos kategoriją.

15. Registro asmens duomenų tvarkymas automatiniu būdu priskirtinas trečiajam saugumo lygiui vadovaujantis Bendrųjų reikalavimų organizacinėms ir techninėms asmens duomenų saugumo priemonėms 11.3 papunkčio nuostatomis.

16. Saugos įgaliotinis, vadovaudamasis Lietuvos Respublikos vidaus reikalų ministerijos metodine priemone „Rizikos analizės vadovas“, Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais, kasmet organizuoja Registro rizikos vertinimą. Prireikus Saugos įgaliotinis gali organizuoti neeilinį Registro rizikos vertinimą. Registro valdytojo rašytiniu pavedimu Registro rizikos vertinimą gali atlikti

pats Saugos įgaliotinis arba Registro rizikos veiksnių vertinimui atlikti gali būti perkamos rizikos vertinimo paslaugos.

17. Registro rizikos veiksnių vertinimui taikoma kokybinė rizikos vertinimo metodika.

18. Registro rizikos vertinimo rezultatai išdėstomi rizikos vertinimo ataskaitoje. Rizikos vertinimo ataskaita rengiama įvertinant rizikos veiksnius, galinčius turėti įtakos Registro duomenų saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausieji rizikos veiksniai yra šie:

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

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

18.3. 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.

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

20. Registro saugos priemonės parenkamos įvertinus galimus rizikos veiksnius Registro duomenų vientisumui, konfidencialumui ir prieinamumui.

21. Pagrindiniai Registro duomenų saugos priemonių parinkimo principai yra šie:

21.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

21.2. Registro duomenų saugos priemonės diegimo kainos atitiktis saugomos informacijos vertei;

21.3. esant galimybei, turi būti įdiegtos prevencinės, detekcinės ir korekcinės Registro duomenų saugos priemonės.

22. Siekiant užtikrinti Saugos nuostatuose ir Registro saugos politiką įgyvendinančiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, vadovaujantis Lietuvos Respublikos vidaus reikalų ministro patvirtinta metodika, kasmet organizuojamas Registro informacinių technologijų saugos atitikties vertinimas, kurio metu:

22.1. įvertinama Saugos nuostatų ir Registro saugos politiką įgyvendinančių dokumentų atitiktis realiai Registro duomenų saugos situacijai;

22.2. inventorizuojama Registro techninė ir programinė įranga;

22.3. patikrinama ne mažiau kaip 10 procentų Registro naudotojų kompiuterizuotų darbo vietų ir Registro tarnybinėse stotyse įdiegtos programos ir jų sąranka (konfigūracija);

22.4. patikrinama (įvertinama) Registro naudotojams suteiktų teisių ir vykdomų funkcijų atitiktis;

22.5. įvertinamas pasiruošimas atkurti Registro veiklą įvykus Registro duomenų saugos incidentui.

23. Registro informacinių technologijų saugos atitikties vertinimą ne rečiau kaip kartą per trejus metus turi atlikti nepriklausomi, visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų auditoriai.

24. Atlikus Registro informacinių technologijų saugos atitikties vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato Registro valdytojas.

25. Registro rizikos vertinimo ataskaitos, rizikos vertinimo ir rizikos valdymo priemonių plano, Registro informacinių technologijų saugos atitikties vertinimo ataskaitos ir pastebėtų trūkumų šalinimo plano kopijas Registro valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2012 m. spalio 16 d. įsakymu Nr. 1V-740 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

## III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

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

26.1. Registro tarnybinėse stotyse ir Registro naudotojų kompiuterinėse darbo vietose privalo būti naudojama programinė įranga, skirta kovai su kenksminga programine įranga, atnaujinama automatiniu būdu ne rečiau kaip kas trys dienos;

26.2. Registro tarnybinėse stotyse ir Registro naudotojų kompiuterinėse darbo vietose neturi veikti programinė įranga, nesusijusi su Registro duomenų tvarkymu;

26.3. Registro naudotojų kompiuterinėse darbo vietose turi būti įdiegtos priemonės, leidžiančios riboti išorinių duomenų laikmenų (USB, CD/DVD ir kt.) naudojimą;

26.4. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

27. Programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos:

27.1. Registro darbui turi būti naudojama tik legali programinė įranga;

27.2. programinė įranga prižiūrima ir nuolat atnaujinama laikantis gamintojo rekomendacijų;

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

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

28.1. Registrui naudojamas Vidaus reikalų telekomunikacinis tinklas (toliau – VRTT), už kurio administravimą ir priežiūrą atsako šio tinklo pagrindinis tvarkytojas, turi būti atskirtas nuo kitų tinklų tinklo užkarda;

28.2. naudojamos turinio filtravimo sistemos;

28.3. naudojamos taikomųjų programų kontrolės sistemos.

29. Leistinos kompiuterių naudojimo ribos ir metodai, kuriais leidžiama užtikrinti saugų Registro duomenų teikimą ir (ar) gavimą:

29.1. tiesioginė prieiga prie Registro duomenų suteikiama įgyvendinus Registro naudotojų autentifikavimo priemones – Registro naudotojai tapatybę patvirtina slaptažodžiu. Registro naudotojų slaptažodžiai sudaromi, keičiami ir jų galiojimo trukmė nustatoma vadovaujantis VRIS CDB naudotojų administravimo taisyklėmis. Tiesioginė prieiga prie Registro duomenų užtikrinama automatiniu būdu visą parą, darbo ir poilsio dienomis;

29.2. Registro duomenys perduodami automatiniu būdu naudojant TCP/IP, HTTP, HTTPS, FTP protokolus realiame laike („On-line“ režimu) arba asinchroniniu režimu pagal duomenų teikimo sutartis, kuriose nustatytos perduodamų duomenų specifikacijos, duomenų perdavimo sąlygos ir tvarka;

29.3. Registro naudotojams, tarnybinėms funkcijoms vykdyti naudojantiems nešiojamuosius kompiuterius Registro duomenų perdavimui kompiuterių tinklais ne savo darbo vietoje, šiuose kompiuteriuose turi būti naudojamas kompiuterio įjungimo slaptažodis, papildomas Registro naudotojo tapatybės patvirtinimas ir Registro duomenų šifravimas;

29.4. Registro naudotojams, kuriems atliekant tiesiogines pareigas būtina prisijungti iš nutolusios darbo vietos, gali būti suteikiama nuotolinio prisijungimo prie Registro galimybė:

29.4.1. Techninis nuotolinio prisijungimo sprendimas turi užtikrinti ne žemesnį nei vidiniam prisijungimui naudojamą saugumo lygį, t. y. turi būti naudojamos Saugos nuostatuose nurodytos priemonės ir Registro duomenų šifravimas naudojantis virtualiu privačiu tinklu (angl. *virtual private network* – VPN);

29.4.2. prie Registro prisijungiama nuotoliniu būdu naudojant interneto naršyklę (HTTPS protokolą);

29.5. užtikrinant saugų Registro duomenų teikimą ir (ar) gavimą, naudojami saugūs ryšio kanalai.

30. Registro atsarginių duomenų kopijų darymo ir atkūrimo reikalavimai nustatyti Vidaus reikalų informacinės sistemos centrinio duomenų banko atsarginių duomenų kopijų darymo, saugojimo ir duomenų atkūrimo iš atsarginių duomenų kopijų tvarkos apraše, patvirtintame Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2012 m. gegužės 2 d. įsakymu Nr. 5V-39 „Dėl Vidaus reikalų informacinės sistemos centrinio duomenų banko atsarginių duomenų kopijų darymo, saugojimo ir duomenų atkūrimo iš atsarginių duomenų kopijų tvarkos aprašo“.

31. Registro duomenys, kurių saugojimo terminas yra pasibaigęs, arba klaidingi Registro duomenys, dėl kurių priimtas teismo sprendimas Registro duomenis sunaikinti, sunaikinami pašalinant įrašą iš Registro duomenų bazės ir (ar) duomenų bazės archyvo. Sunaikinimas įforminamas duomenų sunaikinimo aktu, kuriame nurodoma:

31.1. naikinimo procedūrą atliekantis (atliekantys) asmuo (asmenys);

31.2. sunaikinamų duomenų apimtis;

31.3. duomenų sunaikinimo teisinis pagrindas.

## IV. REIKALAVIMAI PERSONALUI

32. Saugos įgaliotinis privalo išmanyti informacinių sistemų administravimą, elektroninės informacijos saugos užtikrinimo principus ir priemones, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų duomenų tvarkymą. Saugos įgaliotinis privalo tobulinti kvalifikaciją elektroninės informacijos saugos srityje.

33. 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.

34. Registro administratorius privalo būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais, išmanyti pagrindinius saugos politikos, darbo su duomenų perdavimo tinklais principus, užtikrinti jų saugą, administruoti ir prižiūrėti Registro duomenų bazę, gebėti užtikrinti techninės ir programinės įrangos nepertraukiamą funkcionavimą, stebėti techninės ir programinės įrangos veikimą, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, sutrikimų diagnostiką ir šalinimą, turėti sisteminių programinių priemonių (*Windows, Unix, Oracle*) administravimo ir priežiūros patirties.

35. Visi Registro naudotojai privalo:

35.1. turėti atitinkamą kvalifikaciją (informacinių technologijų vartotojų kvalifikacijos kursai, pradinis saugaus darbo su duomenimis mokymas, ECDL (Europos kompiuterio vartotojo pažymėjimas) vartotojo sertifikatas ar pan.) ir patirties (dirbant su atitinkamomis operacinėmis sistemomis, taikomosiomis programomis ir pan.);

35.2. turi būti susipažinę su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, kitais teisės aktais, reglamentuojančiais asmens duomenų tvarkymą ir Registro duomenų saugą;

35.3. pasirašę pasižadėjimą saugoti asmens duomenų paslaptį;

35.4. nuolat kelti kvalifikaciją kvalifikacijos kėlimo kursuose, saugaus darbo su duomenimis seminaruose.

36. Registro naudotojams turi būti nuolat rengiami duomenų saugos mokymai, įvairiomis priemonėmis (elektroniniu paštu, pateikdamas atmintines naujai priimtiems darbuotojams, organizuodamas teminius seminarus) primenama apie saugos problematiką.

## V. REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

37. Už Registro naudotojų supažindinimą su Saugos nuostatais ir Registro saugos politiką įgyvendinančiais dokumentais ir atsakomybe už šių reikalavimų nesilaikymą organizuoja Saugos įgaliotinis. Saugos įgaliotinis raštu informuoja Registro naudotojus apie Saugos nuostatų pakeitimus ar Registro saugos politiką įgyvendinančių dokumentų pripažinimą netekusiais galios, keitimą ar priėmimą.

38. Saugos nuostatai ir Registro saugos politiką įgyvendinantys dokumentai skelbiami Registro valdytojo interneto svetainėje.

39. Registro naudotojai su Saugos nuostatais ir kitais Registro saugos politiką įgyvendinančiais dokumentais ir atsakomybe už jų reikalavimų nesilaikymą supažindinami pasirašytinai.

## VI. BAIGIAMOSIOS NUOSTATOS

40. Saugos įgaliotinis, Registro administratorius ir Registro naudotojai privalo saugoti Registro duomenų paslaptį. Įsipareigojimas saugoti Registro duomenų paslaptį galioja ir nutraukus su Registro duomenų tvarkymu susijusią veiklą.

41. Saugos įgaliotinis, Registro administratorius ir Registro naudotojai, pažeidę Saugos nuostatų ir Registro saugos politiką įgyvendinančių dokumentų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

---

**Pakeitimai:**

1.
Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos, Įsakymas
Nr. 5V-49, 2015-09-24, paskelbta TAR 2015-09-24, i. k. 2015-14176
Dėl Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2012 m. liepos 4 d. įsakymo Nr. 5V-57 „Dėl Įtariamųjų, kaltinamųjų ir nuteistųjų registro duomenų saugos nuostatų patvirtinimo“ pakeitimo

2.
Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos, Įsakymas
Nr. 5V-1, 2016-01-05, paskelbta TAR 2016-01-05, i. k. 2016-00079
Dėl Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2012 m. liepos 4 d. įsakymo Nr. 5V-57 „Dėl Įtariamųjų, kaltinamųjų ir nuteistųjų registro duomenų saugos nuostatų patvirtinimo“ pakeitimo