LIETUVOS RESPUBLIKOS KONKURENCIJOS TARYBOS
PIRMININKAS

ĮSAKYMAS
DĖL SUTEIKTOS VALSTYBĖS PAGALBOS IR NEREIKŠMINGOS (*DE MINIMIS*) PAGALBOS REGISTRO BEI KITŲ KONKURENCIJOS TARYBOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2021 m. gegužės d. Nr. 2V-
Vilnius

Vadovaudamasis Lietuvos Respublikos konkurencijos įstatymo 55 straipsnio 3 dalimi, Lietuvos Respublikos valstybes informacinių išteklių valdymo įstatymo 43 straipsnio 2 dalimi ir 3 dalimis, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybes 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“ 11 ir 19 punktais:

1. T v i r t i n u Suteiktos valstybės pagalbos ir nereikšmingos (*de minimis*) pagalbos registro bei kitų Konkurencijos tarybos informacinių sistemų duomenų saugos nuostatus (pridedama).

2. S k i r i u Konkurencijos tarybos patarėją Martyną Plikusą Suteiktos valstybės pagalbos ir nereikšmingos (*de minimis*) pagalbos registro bei kitų Konkurencijos tarybos informacinių sistemų saugos įgaliotiniu.

3. P a v e d u Administracijos direktoriui užtikrinti, kad ne vėliau kaip per 6 mėnesius nuo Suteiktos valstybės pagalbos ir nereikšmingos (*de minimis*) pagalbos registro bei kitų Konkurencijos tarybos informacinių sistemų duomenų saugos nuostatų patvirtinimo būtų parengti ir pateikti tvirtinti Konkurencijos tarybos pirmininkui Suteiktos valstybės pagalbos ir nereikšmingos (*de minimis*) pagalbos registro bei kitų Konkurencijos tarybos informacinių sistemų duomenų saugos politiką įgyvendinančių dokumentų projektai.

4. P r i p a ž į s t u netekusiu galios Lietuvos Respublikos konkurencijos tarybos pirmininko 2016 m. rugsėjo 6 d. įsakymą Nr. 2V-20 „Dėl Suteiktos valstybės pagalbos ir nereikšmingos (*de minimis*) pagalbos registro duomenų saugos nuostatų patvirtinimo“ su visais pakeitimais ir papildymais.

Pirmininkas Šarūnas Keserauskas

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2021 m. gegužės 17 d. raštu Nr.(4.1 E) 6K-392

PATVIRTINTA
Lietuvos Respublikos konkurencijos tarybos
pirmininko 2021 m. gegužės d.
įsakymu Nr. 2V-

SUTEIKTOS VALSTYBĖS PAGALBOS IR NEREIKŠMINGOS (*DE MINIMIS*) PAGALBOS REGISTRO BEI KITŲ KONKURENCIJOS TARYBOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Suteiktos valstybės pagalbos ir nereikšmingos (*de minimis*) pagalbos registro bei kitų Konkurencijos tarybos informacinių sistemų duomenų saugos nuostatai (toliau kartu – Saugos nuostatai) reglamentuoja Suteiktos valstybės pagalbos ir nereikšmingos (*de minimis*) pagalbos registro (toliau – Registras) bei kitų Konkurencijos tarybos informacinių sistemų (toliau – Informacinių sistemų) elektroninės informacijos saugos politiką, kurios tikslas – nustatyti ir įgyvendinti organizacines, technines ir kitas priemones, suteikiančias galimybę saugiai tvarkyti elektroninę informaciją ir užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo ar neteisėto tvarkymo.

2. Saugos nuostatuose vartojamos sąvokos atitinka 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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Bendrųjų saugos reikalavimų aprašas), Suteiktos valstybės pagalbos ir nereikšmingos (*de minimis*) pagalbos registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2005 m. sausio 19 d. nutarimu Nr. 35 „Dėl suteiktos valstybės pagalbos ir nereikšmingos (*de minimis*) pagalbos registro nuostatų patvirtinimo“ (toliau – Registro nuostatai), vartojamas sąvokas.

3. Registro ir Informacinių sistemų elektroninės informacijos saugos tikslas – užtikrinti Registro ir Informacinių sistemų elektroninės informacijos konfidencialumą, prieinamumą, vientisumą bei sudaryti sąlygas saugiai automatiniu būdu tvarkyti Registro ir Informacinių sistemų elektroninę informaciją.

4. Elektroninės informacijos saugos politika įgyvendinama pagal šiuos Saugos nuostatus ir kitus Konkurencijos tarybos pirmininko tvirtinamus saugos politiką įgyvendinančius dokumentus: Registro ir Informacinių sistemų saugaus elektroninės informacijos tvarkymo taisykles, Registro ir Informacinių sistemų naudotojų administravimo taisykles, Registro ir Informacinių sistemų veiklos tęstinumo valdymo planą (toliau visi kartu – saugos dokumentai).

5. Registro ir Informacinių sistemų elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

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

5.2. Registre ir Informacinėse sistemose tvarkomų asmens duomenų apsauga;

5.3. Registro ir Informacinių sistemų veikos tęstinumo užtikrinimas.

6. Saugos nuostatų reikalavimai taikomi:

6.1. Registro ir Informacinių sistemų valdytojui bei tvarkytojui – Lietuvos Respublikos konkurencijos tarybai, Jogailos g. 14, LT-01116 Vilnius;

6.2. Registro ir Informacinių sistemų saugos įgaliotiniui (toliau – Saugos įgaliotinis);

6.3. Registro ir Informacinių sistemų administratoriams (toliau kartu – Sistemų administratoriai);

6.4. Registro ir Informacinių sistemų naudotojams (toliau kartu – Sistemų naudotojai).

7. Sistemų administratorių funkcijas pagal kompetenciją vykdo Konkurencijos tarybos pirmininko paskirti Konkurencijos tarybos darbuotojai (vietinis (-iai) administratorius (-iai) ir Registro naudotojų administratorius (-iai) ir, pagal poreikį, paslaugų teikėjas (-ai), su kuriuo(-iais) Konkurencijos taryba yra sudariusi paslaugų teikimo sutartį (-is) Viešųjų pirkimų įstatymo nustatyta tvarka.

8. Konkurencijos taryba, kaip Registro ir Informacinių sistemų valdytoja bei tvarkytoja atlieka šias funkcijas:

8.1. formuoja saugos politiką ir organizuoja jos įgyvendinimą, priežiūrą, ir atsako už elektroninės informacijos tvarkymo teisėtumą;

8.2. atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka;

8.3. skiria Saugos įgaliotinį bei Sistemų administratorius (vietinį (-ius) administratorių (-ius) ir Registro naudotojų administratorių (-ius)), sudaro sutartis dėl saugos įgaliotinių ir (ar) Sistemų administratorių paslaugų įsigijimo;

8.4. vykdo kitas Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Registro nuostatuose bei saugos dokumentuose nustatytas funkcijas.

9. Saugos įgaliotinio funkcijos ir atsakomybė:

9.1. prižiūri Registro ir Informacinių sistemų elektroninės informacijos saugos politikos įgyvendinimą;

9.2. teikia Konkurencijos tarybos pirmininkui siūlymus dėl:

9.2.1. vietinio administratoriaus ir Registro naudotojų administratoriaus paskyrimo bei reikalavimų jiems nustatymo, pagal poreikį, inicijuoja ir organizuoja viešuosius pirkimus dėl Sistemų administratorių paslaugų įsigijimo;

9.2.2. Konkurencijos tarybos informacinių technologijų saugos atitikties vertinimo atlikimo;

9.2.3. Registro ir Informacini sistemų saugos dokumentų priėmimo, keitimo.

9.3. koordinuoja Registro ir Informacinių sistemų saugos incidentų, įvykusių informacinėje sistemoje, tyrimą ir bendradarbiauja su kompetentingoms institucijoms, 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;

9.4. organizuoja Registro ir Informacinių sistemų rizikos įvertinimą;

9.5. ne rečiau kaip kartą per metus organizuoja saugos dokumentų svarstymą (peržiūrėjimą);

9.6. teikia Sistemų administratoriams ir Sistemų naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos politikos įgyvendinimu;

9.7. supažindina Sistemų administratorius bei Sistemų naudotojus su Registro ir Informacinių sistemų saugos politiką įgyvendinančių dokumentų reikalavimais, atsakomybe už šių dokumentų reikalavimų nesilaikymą, organizuoja Sistemų naudotojų mokymą elektroninės informacijos saugos klausimais, informuoja juos apie elektroninės informacijos saugos problemas;

9.8. atlieka kitas Saugos nuostatuose ir teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą, nustatytas funkcijas.

10. vietinis administratorius atlieka funkcijas, susijusias su šiais Registro ir Informacinių sistemų komponentais – kompiuteriais, operacinėmis sistemomis, ugniasienėmis, įsilaužimų aptikimo sistemomis, elektroninės informacijos perdavimu tinklais, serveriais ir kitais.

11. Registro naudotojų administratorius atlieka funkcijas, susijusias išskirtinai su Registro naudotojų teisių valdymu ir Registro naudotojų konsultavimu.

12. Sistemų administratorius (-iai), su kuriuo (-iais) Konkurencijos taryba yra sudariusi paslaugų teikimo sutartį (-is), atlieka funkcijas, susijusias su šiais Registro ir Informacinių sistemų komponentais – duomenų bazių valdymo sistemomis, taikomųjų programų sistemomis, kibernetinio saugumo užtikrinimu.

13. Visi Sistemų administratoriai privalo vykdyti Saugos įgaliotinio nurodymus ir pavedimus, susijusius su Registro ir Informacinių sistemų saugos užtikrinimu, nuolat teikti Saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę, taip pat bendrai atlieka funkcijas, susijusias su:

13.1. Registro ir Informacinių sistemų komponentų sąranka;

13.2. Registro ir Informacinių sistemų pažeidžiamų vietų nustatymu;

13.3. saugumo reikalavimų atitikties nustatymu ir stebėsena;

13.4. reagavimu į elektroninės informacijos saugos incidentus.

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

14.1. Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

~~14.2.~~ Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

14.3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

14.4. Lietuvos Respublikos kibernetinio saugumo įstatymas;

14.5. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

14.6. Bendrųjų saugos reikalavimų aprašas;

14.7. Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymas 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“;

14.8. Registro nuostatai;

14.9. Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, nustatantys saugų elektroninės informacijos tvarkymą;

14.10. Valstybinės duomenų apsaugos inspekcijos rekomendacijos ir gairės, reglamentuojančios asmens duomenų tvarkymą ir saugumo užtikrinimą;

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

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

15. Registre ir Informacinėse sistemose tvarkoma elektroninė informacija priskiriama vidutinės svarbos informacijos kategorijai, 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 – Klasifikavimo gairių aprašas) 9.1 ir 9.2 papunkčių nuostatomis.

16. Registras ir Informacinės sistemos priskiriamos trečiajai kategorijai, vadovaujantis Klasifikavimo gairių aprašo 12.3 papunkčio nuostatomis, atsižvelgiant į Registre apdorojamos elektroninės informacijos svarbos kategoriją.

17. Saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro prie Lietuvos Respublikos krašto apsaugos ministerijos interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“, grupės standartus, vidinius rizikos valdymą reglamentuojančius dokumentus, kasmet organizuoja Registro ir Informacinių sistemų rizikos įvertinimą. Prireikus Saugos įgaliotinis gali organizuoti neeilinį Registro ir Informacinių sistemų rizikos įvertinimą. Registro ir Informacinių sistemų rizikos įvertinimui gali būti įsigyjamos išorinės rizikos vertinimo paslaugos Viešųjų pirkimų įstatymo nustatyta tvarka. Einamaisiais metais įsigijus išorines rizikos vertinimo paslaugas savarankiškas rizikos vertinimas neatliekamas.

18. Registro ir Informacinių sistemų rizikos įvertinimo ataskaitos rengiamos atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausieji rizikos veiksniai yra šie:

18.1. 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, netinkamas veikimas ir kita);

18.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis Registru ar Informacinėmis sistemomis elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo 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. Rizikos įvertinimo ataskaitos ir rizikos valdymo priemonių plano duomenis bei jų kopijas Konkurencijos taryba ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų patvirtinimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai (toliau – ARSIS).

20. Siekiant įvertinti Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, kartą per metus Saugos įgaliotinis organizuoja Registro ir Informacinių sistemų informacinių technologijų saugos reikalavimų atitikties vertinimą. Registro ir Informacinių sistemų atitikties įvertinimui gali būti įsigyjamos išorinės atitikties vertinimo paslaugos Viešųjų pirkimų įstatymo nustatyta tvarka. Einamaisiais metais įsigijus išorines atitikties vertinimo paslaugas savarankiškas rizikos vertinimas neatliekamas.

21. Atlikęs Registro ir Informacinių sistemų informacinių technologijų saugos reikalavimų atitikties vertinimą, Saugos įgaliotinis parengia ir Konkurencijos tarybos pirmininkui bei administracijos direktoriui teikia Registro ir Informacinių sistemų saugos atitikties vertinimo ataskaitą ir pastebėtų trūkumų šalinimo planą, kuriame nurodomi atsakingi vykdytojai ir nustatomi numatytų priemonių įgyvendinimo terminai.

22. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas Konkurencijos taryba ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų patvirtinimo pateikia ARSIS, jos nuostatų nustatyta tvarka.

23. Elektroninės informacijos saugos būklė gerinama techninėmis, programinėmis ir organizacinėmis saugos priemonėmis, kurios pasirenkamos atsižvelgiant į Konkurencijos tarybos skiriamus išteklius, vadovaujantis šiais principais:

23.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

23.2. saugos priemonės diegimo kaina turi atitikti saugomos elektroninės informacijos vertę;

23.3. esant galimybei, turi būti įdiegiamos prevencinės elektroninės informacijos saugos priemonės.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

24. Registro ir Informacinių sistemų tarnybinėse stotyse bei kompiuterizuotose darbo vietose turi būti naudojamos kenksmingos programinės įrangos aptikimo priemonės, nuolat ieškančios ir blokuojančios kenksmingą programinę įrangą (virusų, šnipinėjimo programinę įrangą ir kt.), kurios turi būti reguliariai atnaujinamos automatiniu būdu ne rečiau kaip kartą per 48 valandas.

25. Programinės įrangos, įdiegtos Registro ir Informacinių sistemų tarnybinėse stotyse bei kompiuterizuotose darbo vietose, naudojimo nuostatos:

25.1. Registro ir Informacinių sistemų darbui turi būti naudojama tik legali programinė įranga;

25.2. programinė įranga atnaujinama laikantis gamintojo reikalavimų;

25.3. Registro ir Informacinių sistemų tarnybinėse stotyse neturi veikti programinė įranga, nesusijusi su Registro ir (ar) Informacinių sistemų duomenų tvarkymu, Sistemų naudotojų ir pačios įrangos administravimu;

25.4. Registro ir Informacinių sistemų programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims;

25.5. Saugos įgaliotinis parengia leistinos programinės įrangos sąrašą, kurį kiekvienais metais peržiūri bei prireikus atnaujina.

26. Registro ir Informacinių sistemų tarnybinių stočių kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kt.) pagrindinės naudojimo nuostatos:

26.1. kompiuterių tinklai nuo viešųjų telekomunikacijų tinklų (interneto) turi būti atskirti ugniasienėmis, DOS ir DDOS atakų prevencijai skirta įranga bei įsilaužimų aptikimo ir prevencijos įranga;

26.2. visas duomenų srautas į internetą ir iš jo yra filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos;

26.3. naudojamos turinio filtravimo sistemos.

27. Metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą:

27.1. Registro ir Informacinių sistemų elektroninė informacija perduodama automatiniu būdu naudojant TCP/IP, HTTPS protokolus realiuoju laiku; iš susijusių registrų elektroninė informacija gaunama tik pagal duomenų teikimo sutartis, kuriose nustatytos perduodamos elektroninės informacijos specifikacijos, perdavimo sąlygos ir tvarka;

27.2. prieiga prie Registro ir Informacinių sistemų suteikiama tik registruotiems Sistemų naudotojams;

27.3. tiesioginė prieiga prie Registro ir Informacinių sistemų elektroninės informacijos suteikiama Sistemų naudotojui savo tapatybę patvirtinus slaptažodžiu. Sistemų naudotojų slaptažodžiai sudaromi, keičiami ir jų galiojimo trukmė nustatoma vadovaujantis Registro ir Informacinių sistemų naudotojų administravimo taisyklėmis. Tiesioginė prieiga prie Registro ir Informacinių sistemų užtikrinama ištisą parą darbo ir poilsio dienomis.

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

29. Sistemų naudotojams, kuriems būtinas prisijungimas tiesioginėms pareigoms atlikti iš nutolusios darbo vietos, gali būti suteikiama nuotolinio prisijungimo prie Registro ir Informacinių sistemų galimybė:

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

29.2. prie Registro ir Informacinių sistemų prisijungiama nuotoliniu būdu naudojant interneto naršyklę (HTTPS protokolą).

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

30.1. Registro ir Informacinių sistemų elektroninės informacijos kopijos turi būti daromos automatiškai bent kartą per parą. Prireikus jas atkurti turi teisę Sistemų administratorius arba Saugos įgaliotinis;

30.2. atkūrimas iš elektroninės informacijos kopijų privalo būti išbandomas ne rečiau kaip 1 kartą per metus;

30.3. elektroninės informacijos kopijos turi būti saugomos kitoje patalpoje nei Registro ir Informacinių sistemų tarnybinės stotys. Elektroninė informacija kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, neleidžiančių panaudoti kopijas neteisėtai atkurti elektroninę informaciją.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

31. Saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, tobulinti kvalifikaciją elektroninės informacijos saugos srityje, savo darbe vadovautis Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą. Saugos įgaliotinis, pažeidęs Saugos nuostatų ar kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

32. Sistemų administratoriai pagal kompetenciją privalo išmanyti elektroninės informacijos saugos principus, mokėti užtikrinti Registro ir Informacinių sistemų duomenų saugą, darbo su duomenų perdavimo tinklais principus, administruoti ir prižiūrėti duomenų bazes, gebėti užtikrinti techninės ir programinės įrangos nepertraukiamą funkcionavimą, stebėti jų veikimą, atlikti jų profilaktinę priežiūrą.

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. Sistemų administratoriai ir Sistemų naudotojai turi būti susipažinę su Registro ir Informacinių sistemų saugos dokumentais bei, pagal kompetenciją, su kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą.

35. Sistemų naudotojai raštu pasirašytinai įpareigojami saugoti asmens duomenų paslaptį.

36. Sistemų naudotojai, pastebėję saugos dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai vietiniam administratoriui ar Saugos įgaliotiniui.

37. Saugos įgaliotinio, Sistemų naudotojų, vietinio administratoriaus ir Registro naudotojų administratoriaus mokymų planavimo, organizavimo ir vykdymo tvarka:

37.1. mokymai elektroninės informacijos saugos klausimais organizuojami Saugos įgaliotiniui, Sistemų naudotojams, vietiniam administratoriui ir Registro naudotojų administratoriui;

37.2. mokymai elektroninės informacijos saugos klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į elektroninės informacijos saugos užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), Sistemų naudotojų ar vietinio administratoriaus ir Registro naudotojų administratoriaus poreikius;

37.3. mokymai gali būti vykdomi tiesioginiu (pvz., paskaitos, seminarai, konferencijos ir kiti teminiai renginiai) ar nuotoliniu būdu (pvz., vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir pan.). Mokymus gali vykdyti Saugos įgaliotinis ar kitas Konkurencijos tarybos darbuotojas, išmanantis elektroninės informacijos saugos užtikrinimo principus, arba elektroninės informacijos saugos mokymų paslaugų teikėjas. Saugos įgaliotinio mokymus gali vykdyti tik aukštos kvalifikacijos elektroninės informacijos saugos mokymų paslaugų teikėjas;

37.4. Sistemų naudotojų mokymai turi būti organizuojami periodiškai, ne rečiau kaip kartą per dvejus metus. Saugos įgaliotinio, vietinio administratoriaus ir Registro naudotojų administratoriaus mokymai turi būti organizuojami pagal poreikį. Už mokymų organizavimą atsakingas Saugos įgaliotinis ar kitas Konkurencijos tarybos pirmininko paskirtas darbuotojas.

V SKYRIUS
SISTEMŲ NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

38. Tvarkyti Registro ir Informacinių sistemų duomenis bei gauti informaciją gali tik Sistemų naudotojai, susipažinę su saugos dokumentais, kuriais vadovaujamasi tvarkant elektroninę informaciją, ir raštu pasirašę pasižadėjimus saugoti asmens duomenų paslaptį. Pakartotinis supažindinimas su minėtais dokumentais vykdomas jiems pasikeitus.

39. Už Sistemų naudotojų supažindinimą su saugos dokumentais ir atsakomybe už šių reikalavimų nesilaikymą atsakingas Saugos įgaliotinis.

40. Saugos nuostatai skelbiami Konkurencijos tarybos interneto svetainėje.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

41. Saugos įgaliotinis, Sistemų administratoriai, Sistemų naudotojai, pažeidę Saugos nuostatų ar kitų saugos politiką įgyvendinančių teisės aktų reikalavimus, atsako Lietuvos Respublikos įstatymų ir kitų teisės aktų nustatyta tvarka.

_____