Suvestinė redakcija nuo 2022-04-29

Įsakymas paskelbtas: TAR 2018-10-10, i. k. 2018-16024

Nauja redakcija nuo 2020-06-23:
Nr. 3D-465, 2020-06-22, paskelbta TAR 2020-06-22, i. k. 2020-13624

LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO MINISTRAS

ĮSAKYMAS DĖL NEKILNOJAMOJO TURTO KADASTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2018 m. spalio 9 d. Nr. 3D-723
Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 8 straipsnio 3 dalimi, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 7.1 papunkčiu, 11, 19 ir 26 punktais, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, 6 punktu:

1. T v i r t i n u Nekilnojamojo turto kadastro duomenų saugos nuostatus (pridedama).

2. P a v e d u valstybės įmonei Registrų centrui:

2.1. paskirti:

2.1.1. Nekilnojamojo turto kadastro duomenų valdymo įgaliotinį;

2.1.2. Nekilnojamojo turto kadastro saugos įgaliotinius;

2.1.3. Nekilnojamojo turto kadastro administratorius;

2.2. per 4 mėnesius nuo šio įsakymo įsigaliojimo parengti ir pateikti Lietuvos Respublikos žemės ūkio ministerijai Nekilnojamojo turto kadastro saugaus elektroninės informacijos tvarkymo taisyklių, Nekilnojamojo turto kadastro veiklos tęstinumo valdymo plano, Nekilnojamojo turto kadastro naudotojų administravimo taisyklių ir Nekilnojamojo turto kadastro pokyčių valdymo tvarkos aprašo projektus.

Žemės ūkio ministras Giedrius Surplys

SUDERINTA
Nacionalinio kibernetikos saugumo centro
prie Krašto apsaugos ministerijos
2018 m. rugsėjo 25 d. raštu Nr. (4.2)6K-598

PATVIRTINTA
Lietuvos Respublikos žemės ūkio ministro
2018 m. spalio 9 d. įsakymu Nr. 3D-723
(Lietuvos Respublikos žemės ūkio ministro
2020 m. birželio 22 d. įsakymo Nr.3D-465
redakcija)

NEKILNOJAMOJO TURTO KADASTRO DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Nekilnojamojo turto kadastro duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Nekilnojamojo turto kadastro (toliau – Kadastras) elektroninės informacijos saugos ir kibernetinio saugumo politiką.

2. Saugos nuostatuose vartojamos sąvokos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, 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 elektroninės informacijos saugos reikalavimų aprašas), ir Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – Techninių elektroninės informacijos saugos reikalavimų aprašas).

Punkto pakeitimai:
Nr. 3D-295, 2022-04-28, paskelbta TAR 2022-04-28, i. k. 2022-08676

3. Saugos nuostatai, Kadastro saugaus elektroninės informacijos tvarkymo taisyklės, Kadastro veiklos tęstinumo valdymo planas, Kadastro naudotojų administravimo taisyklės (toliau visi kartu – saugos dokumentai) taikomos:

3.1. Lietuvos Respublikos žemės ūkio ministerijai (Gedimino pr. 19, 01103 Vilnius) – Kadastro valdytojai;

3.2. valstybės įmonei Registrų centrui (toliau – Registrų centras) (Lvovo g. 25-101, 09320 Vilnius) – Kadastro tvarkytojai;

3.3. Kadastro saugos įgaliotiniui (-iams);

3.4. Kadastro administratoriams;

3.5. Kadastro naudotojams;

3.6. Kadastrui funkcionuoti reikalingų paslaugų teikėjams.

4. Saugos nuostatai yra vieši ir skelbiami Teisės aktų registre.

5. Kadastro saugaus elektroninės informacijos tvarkymo taisyklių, Kadastro veiklos tęstinumo valdymo plano, Kadastro naudotojų administravimo taisyklių (toliau visi kartu – saugos politiką įgyvendinantys dokumentai) naudojimas yra ribojamas. Kadastro naudotojams, Kadastrui funkcionuoti reikalingų paslaugų teikėjams ir kitiems tretiesiems

asmenims suteikiama teisė susipažinti tik su jų santrauka Saugos nuostatų V skyriuje nustatyta tvarka.

6. Saugos politiką įgyvendinančių dokumentų santrauka rengiama vadovaujantis būtinumo žinoti principu. Saugos politiką įgyvendinančių dokumentų santrauką rengia Kadastro saugos įgaliotinis, jeigu skiriami keli Kadastro saugos įgaliotiniai – koordinuojantis Kadastro saugos įgaliotinis. Saugos politiką įgyvendinančių dokumentų santrauka derinama su Kadastro valdytoju.

7. Elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo prioritetinės kryptys:

7.1. elektroninės informacijos saugos – elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo – užtikrinimas;

7.2. Kadastro kibernetinio saugumo užtikrinimas;

7.3. asmens duomenų apsauga;

7.4. Kadastro naudotojų mokymas.

8. Elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo tikslai:

8.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti Kadastro elektroninę informaciją;

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

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

9. Kadastro valdytojo funkcijos:

9.1. atlikti Lietuvos Respublikos nekilnojamojo turto kadastro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2002 m. balandžio 15 d. nutarimu Nr. 534 „Dėl Lietuvos Respublikos nekilnojamojo turto kadastro nuostatų patvirtinimo“ (toliau – Kadastro nuostatai), nustatytas funkcijas;

9.2. tvirtinti saugos dokumentus ir kitus teisės aktus, susijusius su Kadastro elektroninės informacijos sauga ir kibernetiniu saugumu;

9.3. koordinuoti Kadastro tvarkytojo darbą įgyvendinant elektroninės informacijos saugos ir kibernetinio saugumo reikalavimus;

9.4. atlikti elektroninės informacijos saugos ir kibernetinio saugumo reikalavimų laikymosi priežiūrą ir kontrolę;

9.5. nagrinėti Kadastro tvarkytojo pasiūlymus dėl elektroninės informacijos saugos ir kibernetinio saugumo tobulinimo ir priimti dėl jų sprendimus;

9.6. skirti Kadastro saugos įgaliotinį (-ius) ir Kadastro administratorius arba pavesti juos paskirti Kadastro tvarkytojui;

9.7. pagal kompetenciją teikti Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos (toliau – Nacionalinis kibernetinio saugumo centras) techninę informaciją, reikalingą Kadastro kibernetiniam saugumui įvertinti, Nacionalinio kibernetinio saugumo centro reikalavimu nurodytais formatais ir terminais arba savo iniciatyva;

9.8. atlikti kitas Saugos nuostatuose ir Saugos nuostatų 24 punkte nurodytuose teisės aktuose nustatytas Kadastro valdytojo funkcijas.

10. Kadastro tvarkytojo funkcijos:

10.1. atlikti Kadastro nuostatuose nustatytas funkcijas;

10.2. užtikrinti saugos dokumentų ir kitų Kadastro valdytojo priimtų teisės aktų, susijusių su Kadastro elektroninės informacijos sauga ir kibernetiniu saugumu, tinkamą įgyvendinimą;

10.3. pagal kompetenciją prižiūrėti Kadastro komponentus (kompiuterius, operacines sistemas ir kitus Kadastro komponentus, nurodytus Saugos nuostatų 19.3 papunktyje), užtikrinti jų veikimą;

10.4. įgyvendinti Kadastro elektroninės informacijos saugos ir kibernetinio saugumo reikalavimus;

10.5. užtikrinti Kadastro elektroninės informacijos saugą ir kibernetinį saugumą;

10.6. teikti Kadastro valdytojui pasiūlymus dėl Kadastro elektroninės informacijos saugos ir kibernetinio saugumo tobulinimo;

10.7. Kadastro valdytojo pavedimu skirti Kadastro saugos įgaliotinį (-ius) ir Kadastro administratorius;

10.8. pagal kompetenciją teikti Nacionaliniam kibernetinio saugumo centrui techninę informaciją, reikalingą Kadastro kibernetiniam saugumui įvertinti, Nacionalinio kibernetinio saugumo centro reikalavimu nurodytais formatais ir terminais arba savo iniciatyva;

10.9. atlikti kitas Saugos nuostatuose ir Saugos nuostatų 24 punkte nurodytuose teisės aktuose nustatytas Kadastro tvarkytojo funkcijas.

11. Už elektroninės informacijos saugą ir kibernetinį saugumą pagal kompetenciją atsako Kadastro valdytojas ir Kadastro tvarkytojas.

12. Kadastro valdytojas atsako už elektroninės informacijos saugos ir kibernetinio saugumo politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą.

13. Kadastro tvarkytojas atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi saugos dokumentuose nustatyta tvarka.

14. Kadastro saugos įgaliotinis ir Kadastro administratorius gali būti paskiriami keliems Kadastro posistemiams, funkciškai savarankiškoms sudedamosioms dalims ar tam tikroms Kadastro saugos įgaliotinio ir Kadastro administratoriaus funkcijoms atlikti.

15. Jeigu skiriami keli Kadastro saugos įgaliotiniai ir (arba) Kadastro administratoriai, teisės akte, kuriuo skiriami Kadastro saugos įgaliotinis (-iai) ir (arba) Kadastro administratoriai, turi būti aiškiai nurodyta:

15.1. kokiam Kadastro posistemiui, funkciškai savarankiškoms sudedamosioms dalims ar kurioms Kadastro saugos įgaliotinio ir (arba) Kadastro administratoriaus funkcijoms atlikti paskiriamas konkretus saugos įgaliotinis ir (arba) administratorius;

15.2. kuriam iš Kadastro saugos įgaliotinių ir (arba) Kadastro administratorių pavedama koordinuoti Kadastro saugos įgaliotinio (-ių) ir (arba) Kadastro administratorių veiklą.

16. Kadastro valdytojas arba Kadastro tvarkytojas, jeigu Kadastro valdytojas jam pavedė skirti Kadastro saugos įgaliotinį (-ius) ir (arba) Kadastro administratorius, turi užtikrinti tinkamą Kadastro saugos įgaliotinio ir Kadastro administratoriaus funkcijų atlikimą (pakankamos žinios, patirtis ir profesinė kvalifikacija, darbo (tarnybos) funkcijų atlikimo vieta sutampa su darbovietės (tarnybos) vieta, funkcijų atskyrimas, siekiant išvengti interesų konfliktų, adekvatus registrų ir (ar) informacinių sistemų, kurių saugos įgaliotiniu ir (arba) administratoriumi skiriamas asmuo, skaičius ir pan.).

17. Kadastro saugos įgaliotinio funkcijos ir teisės:

17.1. koordinuoti ir prižiūrėti elektroninės informacijos saugos ir kibernetinio saugumo politikos įgyvendinimą saugos dokumentuose nustatyta tvarka;

17.2. teikti Kadastro valdytojo vadovui pasiūlymus dėl:

17.2.1. saugos dokumentų priėmimo, keitimo;

17.2.2. informacinių technologijų saugos atitikties vertinimo atlikimo pagal Informacinių technologijų saugos atitikties vertinimo metodiką, patvirtintą Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – Informacinių technologijų saugos atitikties vertinimo metodika);

Papunkčio pakeitimai:
Nr. 3D-295, 2022-04-28, paskelbta TAR 2022-04-28, i. k. 2022-08676

17.3. organizuoti rizikos ir informacinių technologijų saugos atitikties įvertinimą;

17.4. koordinuoti elektroninės informacijos saugos incidentų ir kibernetinių incidentų tyrimą ir bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, elektroninės informacijos saugos incidentus ir kibernetinius incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais ir kibernetiniais incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos ir kibernetinio saugumo darbo grupės;

17.5. teikti Kadastro administratoriams ir Kadastro naudotojams privalomus vykdyti nurodymus ir pavedimus dėl elektroninės informacijos saugos ir kibernetinio saugumo politikos įgyvendinimo;

17.6. turi teisę pagal savo įgaliojimus duoti privalomus vykdyti nurodymus ir pavedimus kitiems Kadastro valdytojo ir Kadastro tvarkytojo tarnautojams ar darbuotojams, dirbantiems pagal darbo sutartį (toliau – darbuotojai), jeigu tai būtina elektroninės informacijos saugos ir kibernetinio saugumo politikai įgyvendinti;

17.7. atlikti Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame 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), nustatytas asmens, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, funkcijas;

17.8. atlikti kitas saugos dokumentuose ir Bendrųjų elektroninės informacijos saugos reikalavimų apraše saugos įgaliotiniui nustatytas funkcijas.

18. Kadastro saugos įgaliotinis negali atlikti Kadastro administratoriaus funkcijų.

19. Kadastro administratoriai pagal atliekamas funkcijas skirstomi į grupes:

19.1. koordinuojantysis administratorius, kuris prižiūri Kadastro administratorių veiklą, siekdamas užtikrinti tinkamą Kadastro administratorių funkcijų vykdymą;

19.2. Kadastro naudotojų administratoriai, kurie atlieka funkcijas, susijusias su Kadastro naudotojų teisių valdymu;

19.3. Kadastro komponentų administratoriai, kurie atlieka funkcijas, susijusias su Kadastro komponentais (kompiuteriais, operacinėmis sistemomis, duomenų bazėmis ir jų valdymo sistemomis, taikomųjų programų sistemomis, ugniasienėmis, įsilaužimų aptikimo ir prevencijos sistemomis, elektroninės informacijos perdavimo tinklais, duomenų saugyklomis, bylų serveriais ir kita technine ir programine įranga, kurios pagrindu funkcionuoja Kadastras ir užtikrinama jame tvarkomos elektroninės informacijos sauga ir kibernetinis saugumas bei Kadastro komponentų sąranka);

19.4. Kadastro saugos administratoriai, kurie atlieka funkcijas, susijusias su Kadastro pažeidžiamų vietų nustatymu, saugumo reikalavimų atitikties nustatymu ir stebėsena.

20. Kadastro administratoriai yra atsakingi už tinkamą saugos dokumentuose jiems nustatytų funkcijų vykdymą.

21. Kadastro administratoriai privalo vykdyti visus Kadastro saugos įgaliotinio nurodymus ir pavedimus dėl Kadastro elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo, pagal kompetenciją reaguoti į elektroninės informacijos saugos ir kibernetinius incidentus ir nuolat teikti Kadastro saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę.

22. Atlikdami Kadastro sąrankos pakeitimus, Kadastro komponentų administratoriai turi laikytis Kadastro pokyčių valdymo tvarkos apraše, tvirtinamame Kadastro valdytojo, nustatytos pokyčių valdymo tvarkos.

23. Kadastro komponentų administratoriai privalo patikrinti (peržiūrėti) Kadastro sąranką ir Kadastro būsenos rodiklius reguliariai – ne rečiau kaip kartą per metus ir (arba) po Kadastro pokyčių, kurių kategorijos nustatomos Kadastro pokyčių valdymo tvarkos apraše.

24. Teisės aktai, kuriais vadovaujamasi tvarkant Kadastro elektroninę informaciją, užtikrinant jos saugą ir kibernetinį saugumą:

24.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos 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) ir kiti Europos Sąjungos teisės aktai, reglamentuojantys asmens duomenų apsaugą;

24.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

24.3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

24.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

24.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

24.6. Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo 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 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);

24.7. Techninių elektroninės informacijos saugos reikalavimų aprašas;

Papunkčio pakeitimai:
Nr. 3D-295, 2022-04-28, paskelbta TAR 2022-04-28, i. k. 2022-08676

24.8. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas;

24.9. Informacinių technologijų saugos atitikties vertinimo metodika;

24.10. Lietuvos standartai LST EN ISO/IEC 27002 ir LST EN ISO/IEC 27001.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

25. Vadovaujantis Klasifikavimo gairių aprašo 7.1–7.3 papunkčių nuostatomis, Kadastre tvarkoma elektroninė informacija priskiriama ypatingos svarbos elektroninės informacijos kategorijai.

26. Vadovaujantis Klasifikavimo gairių aprašo 12.1 papunkčiu, Kadastras pagal jame tvarkomos elektroninės informacijos svarbą priskiriamas pirmajai – aukščiausiajai kategorijai.

27. Rizikos vertinimo organizavimas:

27.1. Kadastro saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo metodai“ grupės standartus, kasmet arba po esminių organizacinių ar sisteminių pokyčių organizuoja Kadastro rizikos įvertinimą. Kadastro rizikos vertinimas gali būti atliekamas kartu su informacinių technologijų saugos atitikties vertinimu. Prireikus Kadastro saugos įgaliotinis gali organizuoti neeilinį Kadastro rizikos įvertinimą. Organizuojant rizikos vertinimą, rekomenduojama Kadastro rizikos vertinimą įtraukti į Kadastro tvarkytojo veiklos rizikos vertinimo procesus;

27.2. organizuojant rizikos vertinimą turi būti paskirtas (-i) už rizikos vertinimą, rizikos vertinimo proceso priežiūrą bei nuolatinį tobulinimą atsakingas (-i) asmuo (-enys), sertifikuotas (-i) Tarptautinės informacinių sistemų audito ir valdymo asociacijos ISACA (angl. *Information Systems Audit and Control Association*) ar kitų visuotinai pripažintų tarptautinių organizacijų. Atsakingu (-ais) asmeniu (-imis), kuris (-ie) atitinka šiame papunktyje nustatytus reikalavimus, gali būti skiriamas (-i) Kadastro valdytojo arba Kadastro tvarkytojo darbuotojas (-ai) arba sudaroma sutartis su rizikos vertinimo, rizikos vertinimo proceso priežiūros bei nuolatinio tobulinimo paslaugas teikiančiu subjektu.

27.3. rizikos vertinimo metu turi būti:

27.3.1. nustatomos grėsmės ir pažeidžiamumai, galintys turėti įtakos Kadastro elektroninės informacijos saugai ir kibernetiniam saugumui;

27.3.2. nustatomos galimos grėsmių ir pažeidžiamumų poveikio vykdomai veiklai sritys;

27.3.3. įvertinama Kadastro pažeidimo grėsmių tikimybė ir pasekmės;

27.3.4. nustatomas rizikos lygis ir įvertinamos identifikuotos grėsmių tikimybės, kurios išdėstomos prioriteto tvarka pagal svarbą, kuri nustatoma atsižvelgiant į atliktą rizikos vertinimą;

27.4. Kadastro rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama Kadastro valdytojo vadovui. Rizikos įvertinimo ataskaita rengiama įvertinant rizikos veiksnius, galinčius turėti įtakos Kadastro elektroninės informacijos saugai ir kibernetiniam saugumui, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Rizikos veiksniai rizikos įvertinimo ataskaitoje išdėstomi pagal prioritetus ir priimtiną rizikos lygį. Svarbiausi rizikos veiksniai yra šie:

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

27.4.2. 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);

27.4.3. 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;

27.5. atsižvelgdamas į rizikos įvertinimo ataskaitą, Kadastro valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti;

27.6. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas Kadastro valdytojas ne vėliau kaip per 5 (penkias) darbo dienas nuo minėtų dokumentų priėmimo pateikia į Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemą Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“ (toliau – Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatai), nustatyta tvarka;

27.7. atsižvelgiant į atlikto rizikos vertinimo rezultatus, taip pat jeigu Saugos nuostatų 28 punkte nustatyta tvarka atliekamo informacinių technologijų saugos atitikties vertinimo metu nustatoma kibernetinių incidentų valdymo ir šalinimo, Kadastro tvarkytojo nepertraukiamos veiklos užtikrinimo trūkumų, atitinkamai turi būti tobulinamas Kadastro veiklos tęstinumo valdymo planas ir (arba) Kibernetinių ir elektroninės informacijos saugos incidentų valdymo tvarkos aprašas. Šių planų veiksmingumo išbandymo rezultatai išdėstomi šių planų veiksmingumo išbandymo ir pastebėtų trūkumų ataskaitose, kurių kopijos ne vėliau kaip per 5 (penkias) darbo dienas nuo šių dokumentų priėmimo pateikiamos Nacionaliniam kibernetinio saugumo centrui.

28. Informacinių technologijų saugos atitikties vertinimo organizavimas:

28.1. informacinių technologijų saugos atitikties vertinimas turi būti organizuojamas siekiant užtikrinti saugos dokumentuose nustatytų elektroninės informacijos saugos ir kibernetinio saugumo reikalavimų įgyvendinimo organizavimą ir kontrolę;

28.2. informacinių technologijų saugos atitikties vertinimas turi būti atliekamas ne rečiau kaip kartą per metus, jei teisės aktuose nenustatyta kitaip. Informacinių technologijų saugos atitikties vertinimą ne rečiau kaip kartą per trejus metus turi atlikti nepriklausomi, visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų auditoriai;

28.3. informacinių technologijų saugos atitikties vertinimas atliekamas Informacinių technologijų saugos atitikties vertinimo metodikoje nustatyta tvarka;

28.4. Kadastro atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus;

28.5. atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos vertinimo ataskaita ir pastebėtų trūkumų šalinimo planas (prireikus), kurie pateikiami Kadastro valdytojo vadovui. Pastebėtų trūkumų šalinimo planą prireikus tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato Kadastro valdytojo vadovas;

28.6. informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas Kadastro valdytojas ne vėliau kaip per 5 (penkias) darbo dienas nuo minėtų dokumentų priėmimo pateikia į Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemą Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

29. Elektroninės informacijos saugos ir kibernetinio saugumo būklės gerinimas:

29.1. techninės, programinės, organizacinės ir kitos Kadastro elektroninės informacijos saugos ir kibernetinio saugumo priemonės pasirenkamos atsižvelgiant į Kadastro valdytojo turimus išteklius, vadovaujantis šiais principais:

29.1.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

29.1.2. priemonės diegimo kaina turi būti adekvati tvarkomos elektroninės informacijos vertei;

29.2. atsižvelgiant į priemonių efektyvumą ir taikymo tikslingumą, turi būti įdiegtos prevencinės, detekcinės ir korekcinės elektroninės informacijos saugos ir kibernetinio saugumo priemonės.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

30. Organizaciniai ir techniniai elektroninės informacijos saugos ir kibernetinio saugumo reikalavimai nustatomi pagal Saugos nuostatų 26 punkte nustatytą Kadastro svarbos kategoriją vadovaujantis Saugos nuostatų 24 punkte nurodytais teisės aktais ir standartais.

31. Kibernetinio saugumo priemonės, nurodytos saugos dokumentuose pagal Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo priedą, turi būti diegiamos atsižvelgiant į naujausius technikos laimėjimus, vadovaujantis gamintojo pateikiama bent viena gerąja saugumo praktikos rekomendacija.

32. Organizacinių ir techninių elektroninės informacijos saugos ir kibernetinio saugumo priemonių užtikrinimas turi būti grindžiamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos Kadastro elektroninės informacijos saugai ir kibernetiniam saugumui, rizikos vertinimu, atsižvelgiant į naujausius technikos laimėjimus.

33. Pagrindiniai organizaciniai ir techniniai elektroninės informacijos saugos ir kibernetinio saugumo reikalavimai:

33.1. detalūs organizaciniai ir techniniai elektroninės informacijos saugos ir kibernetinio saugumo reikalavimai nustatomi saugos politiką įgyvendinančiuose dokumentuose;

33.2. turi būti naudojama ir operatyviai atnaujinama programinė įranga, skirta apsaugoti informacinę sistemą nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamų elektroninių laiškų ir pan.). Detalios šios programinės įrangos naudojimo nuostatos ir jos atnaujinimo reikalavimai (ilgiausias leistinas programinės įrangos neatnaujinimo laikas ir kita) nustatomi Kadastro saugaus elektroninės informacijos tvarkymo taisyklėse;

33.3. Kadastro techninėje įrangoje ir vidinių Kadastro naudotojų kompiuteriuose turi būti naudojama tik legali programinė įranga. Detalios programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos, jos atnaujinimo reikalavimai nustatomi Kadastro saugaus elektroninės informacijos tvarkymo taisyklėse;

33.4. turi būti naudojama kompiuterių tinklo filtravimo įranga (užkardos, turinio kontrolės sistemos, įgaliotieji serveriai (angl. *proxy*) ir kita). Detalios kompiuterių tinklo filtravimo įrangos naudojimo nuostatos nustatomos Kadastro saugaus elektroninės informacijos tvarkymo taisyklėse;

33.5. užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą, turi būti naudojamas šifravimas, virtualus privatus tinklas, skirtinės linijos, saugus elektroninių ryšių tinklas ar kitos priemonės, kuriomis užtikrinamas saugus elektroninės informacijos perdavimas. Metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą (nuotolinio prisijungimo prie Kadastro būdai, protokolai, elektroninės informacijos keitimosi formatai, šifravimo, elektroninės informacijos kopijų skaičiaus reikalavimai, reikalavimai teikti ir (ar) gauti elektroninę informaciją automatiniu būdu tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas ir panašiai), nustatyti Kadastro saugaus elektroninės informacijos tvarkymo taisyklėse;

33.6. stacionarius kompiuterius leidžiama naudoti tik Kadastro valdytojo ir Kadastro tvarkytojo patalpose. Nešiojamiesiems kompiuteriams, išnešamiems iš Kadastro valdytojo ar Kadastro tvarkytojo patalpų, turi būti taikomos papildomos saugos priemonės (elektroninės informacijos šifravimas, prisijungimo ribojimas ir panašiai).

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

34.1. atsarginių elektroninės informacijos kopijų darymo strategija turi būti pasirenkama atsižvelgiant į priimtiną elektroninės informacijos praradimą (angl. *recovery point objective*) ir priimtiną Kadastro neveikimo laikotarpį (angl. *recovery time objective*);

34.2. atsarginės elektroninės informacijos kopijos turi būti daromos ir saugomos tokia apimtimi, kad Kadastro veiklos sutrikimo, elektroninės informacijos saugos incidento, kibernetinio incidento ar elektroninės informacijos vientisumo praradimo atvejais neveikimo laikotarpis nebūtų ilgesnis nei teisės aktais nustatytas Kadastro svarbos kategorijai, nurodytai Saugos nuostatų 26 punkte, o elektroninės informacijos praradimas atitiktų priimtinumo kriterijus;

34.3. atsarginės elektroninės informacijos kopijos turi būti daromos automatiškai periodiškai, bet ne rečiau nei nustatyta Kadastro saugaus elektroninės informacijos tvarkymo taisyklėse;

34.4. elektroninė informacija atsarginėse elektroninės informacijos kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo atsarginių elektroninės informacijos kopijų) arba turi būti imtasi kitų priemonių, dėl kurių nebūtų galima neteisėtai atkurti elektroninės informacijos;

34.5. atsarginių elektroninės informacijos kopijų laikmenos turi būti žymimos taip, kad jas būtų galima identifikuoti, ir saugomos nedegioje spintoje kitose patalpose nei yra Kadastro tarnybinės stotys ar įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate;

34.6. periodiškai, bet ne rečiau kaip kartą per pusmetį, turi būti atliekami elektroninės informacijos atkūrimo iš atsarginių kopijų bandymai;

34.7. patekimas į patalpas, kuriose saugomos atsarginės elektroninės informacijos kopijos, turi būti kontroliuojamas Kadastro saugaus elektroninės informacijos tvarkymo taisyklėse nustatyta tvarka.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

35. Kadastro naudotojų, Kadastro administratorių, Kadastro saugos įgaliotinio kvalifikaciniai reikalavimai:

35.1. visi Kadastro naudotojai privalo turėti pagrindinių darbo kompiuteriu, taikomosiomis programomis įgūdžių, mokėti tvarkyti elektroninę informaciją, būti susipažinę su teisės aktais, reglamentuojančiais asmens duomenų tvarkymą, Kadastro elektroninės informacijos tvarkymą. Asmenys, tvarkantys duomenis ir informaciją, privalo laikyti jų paslaptį ir būti pasirašę pasižadėjimą saugoti duomenų ir informacijos paslaptį. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą;

35.2. Kadastro saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo principus, tobulinti kvalifikaciją elektroninės informacijos saugos ir kibernetinio saugumo srityje, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo ir kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų, reglamentuojančių elektroninės informacijos saugą ir kibernetinį saugumą, nuostatomis. Kadastro tvarkytojas turi sudaryti sąlygas Kadastro saugos įgaliotiniui kelti kvalifikaciją. Kadastro saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikalstamas veikas, nurodytas Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.

35.3. Kadastro administratoriai pagal kompetenciją privalo išmanyti elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo principus, mokėti užtikrinti informacinių sistemų ir jose tvarkomos elektroninės informacijos saugą ir kibernetinį saugumą, administruoti ir prižiūrėti informacinių sistemų komponentus (stebėti informacinių sistemų komponentų veikimą, atlikti jų profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, sugebėti užtikrinti informacinių sistemų komponentų nepertraukiamą funkcionavimą ir pan.).

36. Kadastro naudotojų ir Kadastro administratorių mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo dažnumo reikalavimai:

36.1. Kadastro naudotojams turi būti įvairiais būdais primenama apie elektroninės informacijos saugos ir kibernetinio saugumo problemas (pavyzdžiui, priminimai elektroniniu paštu, teminių renginių organizavimas, atmintinės naujiems Kadastro naudotojams, Kadastro administratoriams ir panašiai);

36.2. mokymai elektroninės informacijos saugos ir kibernetinio saugumo klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), Kadastro saugos įgaliotinio, Kadastro naudotojų ar Kadastro administratorių poreikius;

36.3. mokymai gali būti vykdomi tiesioginiu (pavyzdžiui: paskaitos, seminarai, konferencijos ir kiti teminiai renginiai) ar nuotoliniu (pavyzdžiui: vaizdo konferencijos, mokomosios medžiagos pateikimas elektroniniu paštu, elektroninėje erdvėje ir panašiai) būdu;

36.4. mokymai Kadastro naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per dvejus metus. Už Kadastro naudotojų mokymų organizavimo koordinavimą atsakingas Kadastro saugos įgaliotinis;

36.5. mokymai Kadastro saugos įgaliotiniui ir Kadastro administratoriams turi būti organizuojami pagal poreikį.

V SKYRIUS
INFORMACINIŲ SISTEMŲ NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

37. Kadastro administratorių supažindinimą su saugos dokumentais, Kadastro naudotojų supažindinimą su Saugos nuostatais ir saugos politiką įgyvendinančių dokumentų santrauka, atsakomybe už saugos dokumentų nuostatų pažeidimus organizuoja Kadastro saugos įgaliotinis.

38. Kadastro naudotojų supažindinimo su Saugos nuostatais ir saugos politiką įgyvendinančių dokumentų santrauka būdai turi būti pasirenkami atsižvelgiant į Kadastro specifiką (pavyzdžiui, Kadastro ir jų naudotojų buvimo vietą, organizacinių ir (ar) techninių priemonių, leidžiančių identifikuoti su Saugos nuostatais ir saugos politiką įgyvendinančių dokumentų santrauka susipažinusį asmenį ir užtikrinančių supažindinimo procedūros įrodomąją (teisinę) galią, panaudojimo galimybes ir panašiai). Kadastro naudotojai su Saugos nuostatais ir saugos politiką įgyvendinančių dokumentų santrauka turi būti supažindinami pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodomumą. Saugos politiką įgyvendinančių dokumentų santrauka išoriniams Kadastro naudotojams skelbiama Registrų centro interneto svetainėje ir (arba) Kadastro taikomosiose programose.

39. Kadastrui funkcionuoti reikalingų paslaugų teikėjus ir kitus trečiuosius asmenis su Saugos nuostatais ir saugos politiką įgyvendinančių dokumentų santrauka, atsakomybe už jų reikalavimų pažeidimus supažindina Kadastro administratorius – Kadastro saugos administratorius.

40. Pakartotinai su saugos dokumentais ar Saugos nuostatais ir saugos politiką įgyvendinančių dokumentų santrauka Saugos nuostatų 37 ir 39 punkte nurodyti asmenys supažindinami tik iš esmės pasikeitus Kadastrui arba elektroninės informacijos saugą ar kibernetinį saugumą reglamentuojantiems teisės aktams.

41. Tvarkyti Kadastro elektroninę informaciją gali tik Kadastro naudotojai, kurie yra susipažinę su Saugos nuostatais ir saugos politiką įgyvendinančių dokumentų santrauka ir sutikę laikytis jų reikalavimų.

42. Kadastro naudotojai atsako už Kadastro ir jame tvarkomos elektroninės informacijos saugą ir kibernetinį saugumą pagal kompetenciją. Kadastro naudotojai, Kadastro administratoriai, Kadastro saugos įgaliotinis ir kiti asmenys, pažeidę saugos dokumentų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

43. Kadastro valdytojas saugos dokumentus gali keisti savo arba Kadastro saugos įgaliotinio iniciatyva. Saugos dokumentai turi būti derinami su Nacionaliniu kibernetinio saugumo centru. Keičiami saugos dokumentai gali būti nederinami su Nacionaliniu kibernetinio saugumo centru tais atvejais, kai atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar elektroninės informacijos saugos politikos ir kibernetinio saugumo politikos nekeičiantys pakeitimai arba taisoma teisės technika. Tokiais atvejais Nacionaliniam kibernetinio saugumo centrui turi būti pateiktos šių dokumentų kopijos.

44. Kadastro valdytojas ir Kadastro tvarkytojas saugos dokumentus turi persvarstyti (peržiūrėti) ne rečiau kaip kartą per kalendorinius metus. Saugos dokumentai turi būti persvarstomi (peržiūrimi) atlikus rizikos įvertinimą ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems Kadastro

valdytojo ar Kadastro tvarkytojo pokyčiams. Persvarsčius (peržiūrėjus) saugos dokumentus, turi būti nustatoma, kuriuos iš juose nustatytų elektroninės informacijos saugos ir kibernetinio saugumo reikalavimų būtina atnaujinti ir (ar) įgyvendinti pirmiausia, siekiant užtikrinti Kadastro saugą ir kibernetinį saugumą.

Pakeitimai:

1.
Lietuvos Respublikos žemės ūkio ministerija, Įsakymas
Nr. 3D-465, 2020-06-22, paskelbta TAR 2020-06-22, i. k. 2020-13624
Dėl žemės ūkio ministro 2018 m. spalio 9 d. įsakymo Nr. 3D-723 „Dėl Nekilnojamojo turto kadastro duomenų saugos nuostatų patvirtinimo“ pakeitimo

2.
Lietuvos Respublikos žemės ūkio ministerija, Įsakymas
Nr. 3D-295, 2022-04-28, paskelbta TAR 2022-04-28, i. k. 2022-08676
Dėl žemės ūkio ministro 2018 m. spalio 9 d. įsakymo Nr. 3D-723 „Dėl Nekilnojamojo turto kadastro duomenų saugos nuostatų patvirtinimo“ pakeitimo