Suvestinė redakcija nuo 2024-01-19

Įsakymas paskelbtas: TAR 2020-05-26, i. k. 2020-11113

Nauja redakcija nuo 2024-01-19:
Nr. 4-23, 2024-01-18, paskelbta TAR 2024-01-18, i. k. 2024-00781

LIETUVOS RESPUBLIKOS EKONOMIKOS IR INOVACIJŲ MINISTRAS

ĮSAKYMAS DĖL LIETUVOS ATVIRŲ DUOMENŲ PORTALO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2020 m. gegužės 26 d. Nr. 4-363
Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 15 straipsnio 1 dalimi, Lietuvos Respublikos kibernetinio saugumo įstatymo 21 straipsnio dalimi ir 22 straipsnio 2 dalimi, Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“, 9 punktu, 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 ir Saugos dokumentų turinio gairių aprašo patvirtinimo“, 7, 11, 19 ir 26 punktais:

1. T v i r t i n u Lietuvos atvirų duomenų portalo duomenų saugos nuostatus (pridedama).

2. P a v e d u Informacinės visuomenės plėtros komitetui:

2.1. per vieną mėnesį nuo Lietuvos atvirų duomenų portalo duomenų saugos nuostatų patvirtinimo dienos paskirti Lietuvos atvirų duomenų portalo saugos įgaliotinį, administratorių ir duomenų valdymo įgaliotinį;

2.2. per 6 mėnesius nuo Lietuvos atvirų duomenų portalo duomenų saugos nuostatų patvirtinimo dienos parengti, nustatyta tvarka suderinti ir pateikti Lietuvos atvirų duomenų portalo valdytojui tvirtinti saugos politiką įgyvendinančių dokumentų projektus:

2.2.1. Lietuvos atvirų duomenų portalo saugaus elektroninės informacijos tvarkymo taisyklių projektą;

2.2.2. Lietuvos atvirų duomenų portalo veiklos tęstinumo valdymo plano projektą;

2.2.3. Lietuvos atvirų duomenų portalo naudotojų administravimo taisyklių projektą.

3. N u s t a t a u, kad šio įsakymo vykdymo kontrolę užtikrina Ekonomikos ir inovacijų ministerijos Skaitmeninės darbotvarkės departamento direktorius.

Energetikos ministras, laikinai einantis
ekonomikos ir inovacijų ministro pareigas Žygimantas Vaičiūnas

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2020-05-19 Nr. (4.1 E) 6K-303

PATVIRTINTA
Lietuvos Respublikos ekonomikos ir inovacijų ministro
2020 m. gegužės 26 d. įsakymu Nr. 4-363
(Lietuvos Respublikos ekonomikos ir inovacijų ministro
2024 m. sausio 18 d. įsakymo Nr. 4-23
redakcija)

LIETUVOS ATVIRŲ DUOMENŲ PORTALO DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos atvirų duomenų portalo duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Lietuvos atvirų duomenų portalo (toliau – Portalas) saugos politiką – Portalo elektroninės informacijos saugos valdymą, organizacinius ir techninius Portalo duomenų saugos reikalavimus, reikalavimus su Portalu dirbančiam personalui, su Portalu dirbančių valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartis (toliau kartu – darbuotojas), supažindinimo su saugos politiką įgyvendinančiais dokumentais taisykles (toliau – Portalo saugos politika). Portalo saugos politika įgyvendinama pagal ekonomikos ir inovacijų ministro tvirtinamus Portalo saugos politiką įgyvendinančius dokumentus – Portalo saugaus elektroninės informacijos tvarkymo taisykles, Portalo naudotojų administravimo taisykles, Portalo veiklos tęstinumo valdymo planą (toliau kartu – saugos dokumentai).

2. Saugos nuostatuose vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas).

3. Portalo saugos politikos tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti Portalo elektroninę informaciją, užtikrinti Portalo elektroninės informacijos konfidencialumą, prieinamumą, vientisumą ir tinkamą techninės, programinės ir ryšių įrangos funkcionavimą, vykdyti elektroninės informacijos saugos ir kibernetinių incidentų (toliau kartu – saugos incidentai) prevenciją.

4. Portalo saugos politikos užtikrinimo prioritetinės kryptys:

4.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų Portalo elektroninės informacijos saugai užtikrinti, įgyvendinimas ir šių priemonių įgyvendinimo kontrolė;

4.2. teisėtas, saugus ir kokybiškas Portalo elektroninės informacijos tvarkymas;

4.3. teisėtas ir saugus Portalo asmens duomenų tvarkymas;

4.4. Portalo veiklos tęstinumo užtikrinimas.

5. Portalo elektroninės informacijos saugumo užtikrinimo tikslai:

5.1. Sudaryti sąlygas saugiai automatiniu būdu tvarkyti Portalo elektroninę informaciją.

5.2. Užtikrinti Portalo elektroninės informacijos konfidencialumą, prieinamumą, vientisumą ir tinkamą techninės, programinės ir ryšių įrangos funkcionavimą.

5.3. Vykdyti saugos incidentų, asmens duomenų saugumo pažeidimų prevenciją, reaguoti į saugos incidentus, asmens duomenų saugumo pažeidimus ir juos operatyviai suvaldyti.

6. Portalo valdytoja – Lietuvos Respublikos ekonomikos ir inovacijų ministerija (Gedimino pr. 38, LT-01104 Vilnius).

7. Portalo tvarkytojas – Informacinės visuomenės plėtros komitetas (Konstitucijos pr. 15-89, LT-09319 Vilnius).

8. Portalo valdytojas atlieka Lietuvos atvirų duomenų portalo nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2020 m. sausio 15 d. nutarimu Nr. 24 „Dėl Lietuvos atvirų duomenų portalo nuostatų patvirtinimo“ (toliau – Portalo nuostatai), nustatytas funkcijas, taip pat:

8.1. tvirtina Saugos nuostatus, saugos dokumentus ir kitus su Portalo elektroninės informacijos sauga susijusius teisės aktus;

8.2. koordinuoja Portalo tvarkytojo darbą įgyvendinant elektroninės informacijos saugos reikalavimus;

8.3. prižiūri ir kontroliuoja, kaip laikomasi teisės aktų, susijusių su Portalo tvarkymu ir asmens duomenų apsauga, reikalavimų;

8.4. nagrinėja Portalo tvarkytojo pasiūlymus dėl Portalo saugos politikos tobulinimo ir priima dėl jų sprendimus;

8.5. atsako už Portalo saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą;

8.6. priima sprendimą dėl Portalo elektroninės informacijos saugos priemonių finansavimo.

9. Portalo tvarkytojas atlieka Portalo nuostatuose nustatytas funkcijas, taip pat:

9.1. atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi saugos dokumentuose nustatyta tvarka;

9.2. atlieka Portalo duomenų bazės techninę priežiūrą ir užtikrina nepertraukiamą Portalo veiklą;

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

9.4. užtikrina, kad Portalo naudotojai, turintys teisę naudotis Portalo duomenimis priskirtoms funkcijoms atlikti, laikytųsi saugos dokumentuose nustatytų reikalavimų;

9.5. organizuoja techninių, programinių priemonių, kurios skirtos Portalui eksploatuoti, prižiūrėti ir plėtoti, įsigijimą, jų įdiegimą ir modernizavimą, Portalo techninės, programinės įrangos priežiūrą ir tobulinimą;

9.6. atsako už Portalo elektroninės informacijos saugumą ir Portalo saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams ir Saugos nuostatams;

9.7. teikia Portalo valdytojui pasiūlymus dėl Portalo saugos politikos tobulinimo;

9.8. užtikrina, kad Portalas būtų tvarkomas vadovaujantis Lietuvos Respublikos įstatymais, Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas), saugos dokumentais ir kitais su Portalo tvarkymu susijusiais teisės aktais.

10. Portalo saugos įgaliotinis, koordinuodamas ir prižiūrėdamas elektroninės informacijos saugos politikos įgyvendinimą, atlieka Bendrųjų elektroninės informacijos saugos reikalavimų apraše nustatytas funkcijas.

11. Portalo administratorius, įgyvendindamas Portalo saugos reikalavimus, atlieka Bendrųjų elektroninės informacijos saugos reikalavimų apraše nustatytas funkcijas.

12. Tvarkant Portalo elektroninę informaciją ir užtikrinant jos saugą, vadovaujamasi šiais teisės aktais:

12.1. Valstybės informacinių išteklių valdymo įstatymu;

12.2. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (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) (toliau – Reglamentas (ES) 2016/679);

12.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

12.4. Lietuvos Respublikos kibernetinio saugumo įstatymu;

12.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu;

12.6. Portalo nuostatais;

12.7. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu 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);

12.8. Lietuvos Respublikos vidaus reikalų ministerijos išleista metodine priemone „Rizikos analizės vadovas“, Lietuvos ir tarptautiniais grupės „Informacijos technologija. Saugumo metodai“ standartais, reglamentuojančiais saugų duomenų tvarkymą;

12.9. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašu;

12.10. Portalo saugos dokumentais ir kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą, Portalo duomenų tvarkymo teisėtumą ir elektroninės informacijos saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

13. Vadovaujantis Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2023 m. liepos 19 d. nutarimu Nr. 576 „Dėl Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašo patvirtinimo“, ir Valstybės informacinių išteklių svarbos vertinimo metodikos, patvirtintos Lietuvos Respublikos ekonomikos ir inovacijų ministro 2023 m. liepos 19 d. įsakymu Nr. 4-418 „Dėl Valstybės informacinių išteklių svarbos vertinimo metodikos patvirtinimo“, III skyriaus nuostatomis, Portale tvarkoma elektroninė informacija yra priskiriama vidutinės svarbos informacinių išteklių rūšiai.

14. Pagrindiniai rizikos veiksniai, galintys turėti įtakos Portalo elektroninės informacijos saugai, yra:

14.1. subjektyvūs netyčiniai (Portalo tvarkymo klaidos ir pasirinkimai, ištrynimas, klaidingas teikimas, fiziniai informacinių technologijų sutrikimai, perdavimo tinklais sutrikimai, programinės įrangos klaidos, netinkamas veikimas ir kita);

14.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis Portalo elektronine informacija, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

14.3. atsitiktinės subjektyvios aplinkybės (darbuotojų praradimas, gaisrai, vandens poveikis, elektros instaliacijos gedimas ir kita);

14.4. nenugalima jėga (*force majeure*).

15. Portalo saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja Portalo rizikos įvertinimą ir parengia rizikos įvertinimo ataskaitą; prireikus jis gali organizuoti neeilinį Portalo rizikos įvertinimą.

16. Portalo tvarkytojas, atsižvelgdamas į Portalo rizikos įvertinimo ataskaitą, prireikus rengia ir tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis Portalo rizikos valdymo priemonėms įgyvendinti.

17. Siekdamas užtikrinti saugos dokumentuose nustatytų reikalavimų įgyvendinimo organizavimą ir įgyvendinimo kontrolę, Portalo saugos įgaliotinis ne rečiau kaip kartą per dvejus metus organizuoja Portalo informacinių technologijų saugos reikalavimų atitikties vertinimą, kurio metu:

17.1. įvertinama faktinės Portalo elektroninės informacijos saugos situacijos atitiktis saugos dokumentų, Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo ir kitų su elektroninės informacijos sauga susijusių teisės aktų reikalavimams;

17.2. patikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų Portalo naudotojų kompiuterizuotų darbo vietų ir visų tarnybinių stočių įdiegta programinė įranga ir jos sąranka;

17.3. patikrinama (įvertinama) Portalo naudotojams ir administratoriams suteiktų teisių atitiktis atliekamoms funkcijoms;

17.4. įvertinamas pasirengimas užtikrinti Portalo veiklos tęstinumą įvykus saugos incidentui.

18. Atlikęs Portalo informacinių technologijų saugos atitikties vertinimą, Portalo saugos įgaliotinis rengia pastebėtų trūkumų šalinimo planą, kurį tvirtina, atsakingus vykdytojus skiria ir nustatytų trūkumų šalinimo įgyvendinimo terminus nustato Portalo tvarkytojas.

19. Portalo elektroninės informacijos saugumo priemonės turi būti parenkamos atsižvelgiant į šių nuostatų 13 punkte išvardytus rizikos veiksnius, galinčius turėti įtakos Portalo elektroninės informacijos saugai.

20. Parenkamos tokios saugos priemonės, kad būtų užtikrintas Portalo veiklos tęstinumas, patiriama kuo mažiau išlaidų ir užtikrinamas saugus ir nenutrūkstamas Portalo veikimas.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

21. Programinės įrangos, skirtos Portalui apsaugoti nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos ir jos atnaujinimo reikalavimai:

21.1. Portalo tarnybinėse stotyse ir kompiuterizuotose darbo vietose turi būti naudojamos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės, nuolat ieškančios ir blokuojančios kenksmingą programinę įrangą (virusus, šnipinėjimo programinę įrangą ir pan.), kurios turi būti reguliariai atnaujinamos automatiniu būdu ne rečiau kaip kartą per parą.

21.2. Programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

21.3. Kenksmingosios programinės įrangos aptikimo priemonės turi veikti nuolat realiu laiku.

22. Programinės įrangos, įdiegtos tarnybinėse stotyse ir kompiuterizuotose darbo vietose, naudojimo nuostatos:

22.1. Portalo veikimui gali būti naudojama tik legali ir patikrinta programinė įranga.

22.2. Programinė įranga atnaujinama laikantis gamintojo reikalavimų.

22.3. Programinę įrangą diegia, šalina ir konfigūruoja Portalo administratorius.

23. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kt.) pagrindinės naudojimo nuostatos:

23.1. Kompiuterių tinklai nuo viešųjų telekomunikacijų tinklų (interneto) turi būti atskirti ugniasienėmis ir įsilaužimų aptikimo ir prevencijos įranga.

23.2. Visas duomenų srautas į internetą ir iš jo yra filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos.

23.3. Naudojamos turinio filtravimo sistemos.

24. Pagrindinės kompiuterių (ypač nešiojamųjų) naudojimo nuostatos:

24.1. Prie Portalo prisijungiama nuotoliniu būdu naudojant interneto naršyklę (HTTPS protokolą).

24.2. Prieigą prie Portalo suteikia, apriboja ir panaikina Portalo administratorius.

24.3. Papildomos nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių saugos priemonės nurodytos Portalo saugaus elektroninės informacijos tvarkymo taisyklėse.

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

25.1. Tiesioginė prieiga prie Portalo elektroninės informacijos suteikiama įgyvendinus Portalo naudotojų administravimo taisyklėse nurodytas Portalo naudotojų autentifikavimo priemones.

25.2. Per metus turi būti užtikrintas ne mažiau kaip 90 proc. laiko Portalo prieinamumas darbo metu darbo dienomis.

25.3. Portalo elektroninė informacija perduodama automatiniu būdu arba asinchroniniu režimu pagal duomenų teikimo sutartis, kuriose nustatytos perduodamos elektroninės informacijos specifikacijos, kopijų skaičius ir kitos elektroninės informacijos perdavimo sąlygos ir tvarka.

25.4. Portalo elektroninė informacija, perduodama ne per Portalo tvarkytojams priklausančius duomenų perdavimo tinklus, privalo būti šifruojama.

25.5. Portalo elektroninei informacijai perduoti naudojamas Saugus valstybinis duomenų perdavimo tinklas arba kitas šifruotas perdavimo kanalas, užtikrinantis saugų elektroninės informacijos perdavimą.

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

26.1. Portalo duomenų bazė yra kopijuojama ir saugoma taip, kad įvykus nenumatytai situacijai Portalo veikla būtų visiškai atkurta darbo dienomis per 16 darbo valandų.

26.2. Bandymą atkurti Portalo elektroninę informaciją bent kartą per metus atlieka Portalo administratoriai. Šio bandymo metu Portalo elektroninė informacija atkuriama taip, kaip ji būtų atkuriama tuo atveju, jei būtų netikėtai prarasti duomenys.

26.3. Atsarginės elektroninės informacijos kopijos saugomos kitame valstybės duomenų centre, negu įkurta Portalo duomenų bazė, esančioje patalpoje.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

27. Portalo saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo nuostatomis, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais elektroninės informacijos saugą, tobulinti kvalifikaciją kvalifikacijos kėlimo kursuose, saugaus darbo su duomenimis seminaruose.

28. Portalo saugos įgaliotinis privalo išmanyti kibernetinio saugumo užtikrinimo principus, tobulinti kvalifikaciją kibernetinio saugumo srityje, savo darbe vadovautis Saugos nuostatais, saugos dokumentais, Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašu, kitais kibernetinį saugumą reglamentuojančiais Lietuvos Respublikos ir Europos Sąjungos teisės aktais.

29. Portalo saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninės informacijos 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 veikimui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo šios nuobaudos paskyrimo praėję mažiau kaip vieni metai.

30. Portalo saugos įgaliotinis negali atlikti administratoriaus funkcijų.

31. Portalo administratoriumi skiriamas darbuotojas, išmanantis darbą su Portalo taikomąja programine įranga ir gebantis atlikti funkcijas, susijusias su Portalo naudotojų teisių valdymu.

32. Portalo administratorius turi būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais ir kontroliuoti paslaugų teikėjų, administruojančių ir prižiūrinčių Portalo techninę ir programinę įrangą, veiklą.

33. Portalo naudotojai privalo turėti darbo kompiuteriu įgūdžių, būti susipažinę su saugos dokumentais. Asmenys, kuriems yra suteikiama teisė tvarkyti asmens duomenis, privalo laikytis Reglamente (ES) 2016/679 bei Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme nustatytų asmens duomenų tvarkymo principų ir reikalavimų.

34. Portalo techninę priežiūrą vykdančių įmonių atsakingi darbuotojai turi atitikti Portalo priežiūros ir (ar) plėtros paslaugų pirkimo dokumentuose nurodytus kvalifikacinius reikalavimus bei vykdyti paslaugų teikimo sutartyse numatytas veiklas. Kai perkamos Portalo priežiūros ir (ar) plėtros paslaugos yra susijusios su prieigos prie Portalo bei jame tvarkomos elektroninės informacijos suteikimu, taikomi šie principai:

34.1. Portalo techninę priežiūrą vykdančių įmonių darbuotojams prieiga suteikiama pagal Portalo naudotojų administravimo taisykles. Portalo techninę priežiūrą vykdančių įmonių darbuotojai yra atsakingi už tinkamą Portalo saugos įgaliotinio informavimą apie pasikeitimus jų įmonėje, galinčius turėti įtakos Portalo techninę priežiūrą vykdančių įmonių darbuotojų prieigos prie Portalo panaikinimui ar keitimui (pvz., nedelsiant pranešti apie tai, kad prieigą prie Portalo turintis darbuotojas nutraukia darbo santykius su Portalo techninę priežiūrą vykdančia įmone).

34.2. Neleidžiama suteikti Portalo techninę priežiūrą vykdančių įmonių darbuotojų prieigos prie Portalo grupinių paskyrų pagrindu.

34.3. Prieš Portalo techninę priežiūrą vykdančių įmonių darbuotojams suteikiant prieigą prie Portalo, atitinkami darbuotojai turi pasirašyti konfidencialumo pasižadėjimus ir papildomai turi būti patvirtinti oficialūs susitarimai tarp Portalo tvarkytojo ir Portalo techninę priežiūrą atliekančių įmonių.

35. Portalo saugos įgaliotinis ne rečiau kaip kartą per dvejus metus inicijuoja Portalo naudotojų mokymą elektroninės informacijos saugos, kibernetinio saugumo ir asmens duomenų

apsaugos klausimais, įvairiais būdais (priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės priimtiems naujiems darbuotojams ir panašiai) informuoja juos apie probleminius elektroninės informacijos saugos, kibernetinio saugumo ir asmens duomenų apsaugos klausimus.

V SKYRIUS
NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

36. Tvarkyti Portalo duomenis gali tik tie Portalo naudotojai, kurie yra susipažinę su saugos dokumentais ir sutikę laikytis juose nustatytų reikalavimų.

37. Portalo administratorių su Saugos nuostatais ir kitais saugos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą pasirašytinai supažindina Portalo saugos įgaliotinis per 10 darbo dienų nuo administratoriaus paskyrimo.

38. Portalo naudotojų supažindinimas su saugos dokumentais, atsakomybe už juose nustatytų reikalavimų nesilaikymą ir informacija apie saugos dokumentų priėmimą, pakeitimą ar pripažinimą netekusiais galios užtikrinamas programinėmis Portalo priemonėmis.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

39. Portalo saugos dokumentai turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per kalendorinius metus. Jie taip pat turi būti persvarstomi (peržiūrimi) atlikus rizikos veiksnių analizę ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams. Saugos įgaliotinis atsakingas už tai, kad Portalo naudotojai būtų informuoti apie saugos dokumentų pakeitimą ir (ar) pripažinimą netekusiais galios.

40. Portalo valdytojas rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano, saugos dokumentų ir jų pakeitimų, saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai.

41. Portalo saugos įgaliotinis, Portalo duomenų valdymo įgaliotinis, Portalo administratorius ir Portalo naudotojai, pažeidę Saugos nuostatų, saugos dokumentų ir kitų elektroninės informacijos saugą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

Pakeitimai:

1.
Lietuvos Respublikos ekonomikos ir inovacijų ministerija, Įsakymas
Nr. 4-23, 2024-01-18, paskelbta TAR 2024-01-18, i. k. 2024-00781
Dėl ekonomikos ir inovacijų ministro 2020 m. gegužės 26 d. įsakymo Nr. 4-363 „Dėl Dokumentų rinkinių portalo duomenų saugos nuostatų patvirtinimo“ pakeitimo