PATVIRTINTA
Lietuvos nacionalinės Martyno Mažvydo bibliotekos generalinio direktoriaus 2018-05-08 įsakymu Nr. B-148

VIRTUALIOS KULTŪROS PAVELDO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. SKYRIUS

BENDROSIOS NUOSTATOS

1. Virtualios kultūros paveldo informacinės sistemos (toliau – VEPIS) duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja VEPIS elektroninės informacijos saugos politiką.
2. Šiuose Saugos nuostatuose vartojamos sąvokos:
   2.1. **VEPIS naudotojai** – VEPIS valdytojo arba VEPIS duomenų teikėjo darbuotojas, dirbantis pagal darbo sutartį, tvarkantis VEPIS elektroninę informaciją;
   2.2. **VEPIS administratorius** – VEPIS valdytojo darbuotojas, dirbantis pagal darbo sutartį, prižiūrintis VEPIS ir (ar) jos infrastruktūrą, užtikrinantis jos veikimą, elektroninės informacijos saugą;
   2.3. **VEPIS saugos įgaliotinis** – VEPIS valdytojo darbuotojas koordinuojantis ir prižiūrintis elektroninės informacijos saugos politikos įgyvendinimą bei atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą (kibernetinio saugumo vadovas);
   2.4. **VEPIS duomenų teikėjai** – institucijos, duomenis teikiančios iš valstybės informacinių sistemų;
   2.5. **VEPIS aptarnavimo paslaugų teikėjas** – fizinis ar juridinis asmuo, kuriam pagal sutartį suteiktos VEPIS techninės priežiūros bei garantinio ir (ar) po garantinio aptarnavimo teisės.
   2.6. **VEPIS paslaugų gavėjai** – visi fiziniai asmenys ir juridinių asmenų atstovai besinaudojantys VEPIS.
3. Kitos saugos nuostatuose vartojamos sąvokos atitinka sąvokas, apibrėžtas Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos asmens duomenų teisinės apsaugos 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“, Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 14 d. įsakymu Nr. IV-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“ (toliau – Techniniai valstybės registrų (kadastrų) žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai), ir kituose teisės aktuose bei Lietuvos „Informacijos technologija. Saugumo metodai“ grupės standartuose.
4. VEPIS elektroninės informacijos saugos tikslas – užtikrinti VEPIS elektroninės informacijos prieinamumą, vientisumą ir konfidencialumą bei tinkamą VEPIS infrastruktūros funkcionavimą.
5. VEPIS elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:
   5.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų VEPIS elektroninės informacijos saugai užtikrinti, įgyvendinimas ir šių priemonių įgyvendinimo kontrolė;
   5.2. elektroninės informacijos saugos priemonių parinkimas projektavimo ir diegimo metu;
   5.3. VEPIS elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;
   5.4. VEPIS veiklos tęstinumo užtikrinimas.
6. Saugos nuostatai taikomi:

6.1. VEPIS valdytojui ir tvarkytojui (toliau – valdytojui) – Lietuvos nacionalinė Martyno Mažvydo biblioteka (Gedimino pr. 51, LT-01504, Vilnius);
6.2. VEPIS duomenų teikėjams;
6.3. VEPIS naudotojams, VEPIS administratoriui(-iams), VEPIS saugos įgaliotiniui, VEPIS aptarnavimo paslaugų teikėjams;

7. VEPIS valdytojo funkcijos ir atsakomybė:
7.1. organizuoti VEPIS veiklą ir jai vadovauti;
7.2. tvirtinti dokumentus susijusius su VEPIS elektroninės informacijos sauga;
7.3. priimti sprendimą dėl VEPIS informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;
7.4. skirti VEPIS saugos įgaliotinį ir pavesti jam organizuoti ir kontroliuoti saugos politikos įgyvendinimą VEPIS;
7.5. nustatyti keliamus reikalavimus VEPIS administratoriui(-ams), skirti jį(-uos) ir pavesti jam (-iems) užtikrinti tinkamą VEPIS infrastruktūros veikimą;
7.6. atsakyti už informacijos tvarkymo VEPIS teisėtumą ir elektroninės informacijos saugą;
7.7. užtikrinti nepertraukiamą VEPIS veikimą;
7.8. užtikrinti tinkamą elektroninės informacijos saugos teisės aktų ir rekomendacijų įgyvendinimą;
7.9. organizuoti VEPIS naudotojams kasmetinius informacijos saugos mokymus;
7.10. vykdyti kitus teisės aktuose nustatytas funkcijas.

8. VEPIS duomenų teikėjų funkcijos ir atsakomybė:
8.1. VEPIS duomenų teikimo veiklą organizuoti atsižvelgiant į šiuos VEPIS saugos nuostatus bei kitus saugų elektroninės informacijos tvarkymą reglamentuojančius dokumentus, nurodytus 11.p .
8.2. rengti ir tvirtinti organizacines elektroninės informacijos saugos kontrolės priemones ir užtikrinti jų laikymąsi;
8.3. diegti elektroninės informacijos saugos technines kontrolės priemones kompiuterinėse darbo vietose;
8.4. atsakyti savo tvarkymo srityje už elektroninės informacijos saugą;
8.5. atlikti kitas teisės aktuose nustatytas funkcijas ir VEPIS valdytojo pavedimus.

9. VEPIS informacijos saugos įgaliotinio funkcijos, atsakomybės ir įgaliojimai:
9.1. teikti Lietuvos nacionalinės Martyno Mažvydo bibliotekos generaliniam direktoriui siūlymus dėl:
9.1.1. VEPIS administratoriaus (-ių) paskyrimo ir reikalavimų jiems nustatymo;
9.1.2. VEPIS informacinių technologijų saugos atitikties vertinimo atlikimo;
9.1.3. VEPIS saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;
9.2. koordinuoti elektroninės informacijos saugos incidentų tyrimą;
9.3. teikti VEPIS administratoriui(-iams) ir VEPIS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;
9.4. atlikdamas savo funkcijas, turi teisę pagal savo įgaliojimus duoti privalomus vykdyti nurodymus ir pavedimus ir kitiems VEPIS valdytojo darbuotojams, jeigu tai būtina saugos politikai įgyvendinti;
9.5. kiekvienais metais organizuoti VEPIS rizikos įvertinimą;
9.6. periodiškai organizuoja VEPIS naudotojų ir administratorių mokymus elektroninės informacijos saugos klausimais.
9.7. atlikti kitas saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas ir kitus Lietuvos nacionalinės Martyno Mažvydo bibliotekos generalinio direktoriaus nurodymus, susijusius su VEPIS elektroninės informacijos sauga.

10. VEPIS administratoriaus(-ių) funkcijos ir atsakomybės:
10.1. tarnybinių stočių administratoriai atsako už VEPIS funkcionavimą užtikrinančios techninės ir programinės įrangos darbo užtikrinimą, prieigos prie VEPIS infrastruktūros išteklių teisių nustatymą;
10.2. pagal kompetenciją rengti pasiūlymus dėl VEPIS priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

10.3. registruoti elektroninės informacijos saugos incidentus, informuoti apie juos VEPIS saugos įgaliotinį ir teikti pasiūlymus dėl minėtų incidentų pašalinimo;

10.4. reguliariai tikrinti (peržiūrėti) VEPIS įrangos sąranką ir jos būsenos rodiklius.

11. Teisės aktai, kuriais vadovaujantis tvarkoma VEPIS elektroninė informacija ir užtikrinamas jos saugumas:

11.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

11.2. Lietuvos Respublikos kibernetinio saugumo įstatymu;

11.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

11.4. Bendrųjų elektroninės informacijos saugos reikalavimu aprašu ir Saugos dokumentu turinio gairių aprašu, patvirtintais Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr.716;

11.5. Techniniu valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832;

11.6. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašu patvirtintu Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387;

11.7. Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms patvirtintiems Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) (Valstybinės duomenų apsaugos inspekcijos direktoriaus 2014 m. gruodžio 18 d. įsakymu Nr. 1T-74(1.12));

11.8. Lietuvos standartais LST EN ISO/IEC 27001:2017, LST EN ISO/IEC 27002:2017, taip pat kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais, apibūdinančiais informacijos saugos valdymą ir saugų duomenų tvarkymą.

11.9. kitais teisės aktais, reglamentuojančiais informacinių sistemų elektroninės informacijos tvarkymą, elektroninės informacijos saugą, kibernetinį saugumą bei informacinių sistemų valdytojo ir tvarkytojo veiklą.

II. SKYRIUS

ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

12. VEPIS tvarkoma elektroninė informacija priskiriama vidutinės svarbos elektroninės informacijos kategorijai vadovaujantis Klasifikavimo gairių aprašo 9.3 ir 9.4 papunkčiuose nustatytais kriterijais.

13. Atsižvelgiant į VEPIS tvarkomos elektroninės informacijos svarbos kategoriją ir vadovaujantis Klasifikavimo gairių aprašo 12.3 papunkčiu, VEPIS priskiriama trečiai informacinės sistemos kategorijai.

14. VEPIS asmens duomenų tvarkymas automatiniu būdu priskirtinas antrajam saugumo lygiui vadovaujantis Bendrųjų reikalavimų asmens duomenų saugumo priemonėms 11.2 papunkčio nuostata.

15. VEPIS saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, ne rečiau kaip kartą per 1 metus, organizuoja VEPIS rizikos įvertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį rizikos įvertinimą. VEPIS rizikos veiksnių vertinimui taikoma kokybinė rizikos vertinimo metodika. Kartu su pagrindiniu VEPIS rizikos vertinimu organizuojamas ir atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos VEPIS kibernetiniam saugumui, vertinimas

16. VEPIS rizikos įvertinimas išdėstomas rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausieji rizikos veiksniai yra šie:

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

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

16.3. nenugalima jėga (force majeure).

17. Lietuvos nacionalinės Martyno Mažvydo bibliotekos generalinis direktorius, atsižvelgdamas į VEPIS rizikos įvertinimo ataskaitą, prireikus tvirtina VEPIS saugos įgaliotinio parengtą rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

18. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas VEPIS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

19. Siekiant užtikrinti Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose išdėstytų nuostatų įgyvendinimo kontrolę, VEPIS saugos įgaliotinis ne rečiau kaip kartą per metus organizuoja VEPIS informacinių technologijų saugos reikalavimų atitikties vertinimą, kurio metu:
    19.1. įvertinama Saugos nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų atitiktis realiai VEPIS duomenų saugos situacijai;
    19.2. inventorizuojama VEPIS valdytojo kompiuterinė techninė ir programinė įranga;
    19.3. tikrinama VEPIS tarnybinėse stotyse bei ne mažiau kaip 10 procentų VEPIS valdytojo kompiuterizuotose darbo vietose įdiegta programinė įranga ir jos sąranka (konfigūracija);
    19.4. peržiūrima VEPIS naudotojams suteiktų teisių ir atliekamų funkcijų atitiktis, prireikus VEPIS naudotojų teisės praplečiamos arba apribojamos;
    19.5. tikrinamos VEPIS paslaugų gavėjams suteiktos teisės;
    19.6. įvertinamas pasirengimas atkurti VEPIS veiklos tęstinumą, įvykus VEPIS duomenų saugos incidentui.

20. Remdamasis atlikto VEPIS informacinių technologijų saugos reikalavimų atitikties vertinimo rezultatais, saugos įgaliotinis parengia ir Nacionalinės bibliotekos generaliniam direktoriui pateikia tvirtinti pastebėtų trūkumų šalinimo planą, kuriame nurodomi atsakingi vykdytojai ir nustatomi numatytų priemonių įgyvendinimo terminai.

21. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas VEPIS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

22. Techninės, programinės ir organizacinės elektroninės informacijos saugos priemonės pasirenkamos, kad būtų užtikrintas VEPIS veiklos tęstinumas, patiriant kuo mažiau išlaidų ir užtikrinamas saugus VEPIS naudotojų darbas.

III. SKYRIUS

ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

23. Programinės įrangos, skirtos apsaugoti VEPIS nuo kenksmingos programinės įrangos naudojimo nuostatos:
    23.1. tarnybinėse stotyse ir kompiuterizuotose darbo vietose naudojamos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės, kurios:
        23.1.1. nuolat ieško ir blokuoja kenksmingą programinę įrangą (virusų, šnipinėjimo programinę įrangą ir kt.);
        23.1.2. kenksmingos programinės įrangos parašai ir paieškos variklis reguliariai atnaujinamas kas 8 val. automatiniu būdu arba inicijavus administratoriui, iš centrinės valdymo sistemos;
    23.2. tarnybinės stotys ir kompiuterizuotose darbo vietos negali būti eksploatuojamos be kenksmingos programinės įrangos aptikimo priemonių, nebent rizikos vertinimo metu nustatyta, kad esama rizika priimtina.

24. VEPIS kompiuterinis tinklas turi būti atskirtas filtravimo įranga nuo viešojo interneto. Tinklo srautas tarp VEPIS ir viešojo interneto turi būti analizuojamas.
25. Atliekant VEPIS administravimo ir elektroninės informacijos tvarkymo darbus mobiliųjų įrenginių naudojimas draudžiamas.
26. Nešiojamiesiems kompiuteriams, išnešamiems iš VEPIS valdytojo ir (ar) tvarkytojo patalpų, turi būti taikomos papildomos saugos priemonės (elektroninės informacijos šifravimas, prisijungimo ribojimas ir pan.).
27. VEPIS elektroninės informacijos perdavimui naudojamas(-i) saugūs šifruoti kanalai.
28. Prieiga prie vidinio tinklo nutolusio administravimo ir/ar priežiūros darbams organizuojama VPN („virtual private network“) pagalba.
29. VEPIS interneto svetainė(-s) privalo būti sukonfigūruota prisilaikant gerų saugumo praktikų reikalavimų, tikrinti gaunamus duomenis, ryšys su vartotojais organizuojamas saugiu šifruotu kanalu, naudojant patikimos sertifikavimo tarnybos išduotus sertifikatus.
30. VEPIS elektroninės informacijos atsarginės kopijos daromos automatiškai. Periodiškai atliekama atsarginių kopijų tinkamumo ir saugojimo kontrolė. Elektroninės informacijos kopijos turi būti saugomos kitoje patalpoje nei VEPIS tarnybinės stotys.

IV. SKYRIUS

REIKALAVIMAI PERSONALUI

31. VEPIS saugos įgaliotinis privalo turėti dokumentais patvirtintą informacinių technologijų specialisto kvalifikaciją, išmanyti informacijos saugos užtikrinimo principus, savo darbe vadovautis saugos reikalavimais bei kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą, standartais ir kitais dokumentais, sugebėti prižiūrėti, kaip įgyvendinama saugos politika.
32. VEPIS 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
33. VEPIS administratoriai privalo išmanyti pagrindinius saugos politikos principus, darbą su duomenų perdavimo tinklais, mokėti užtikrinti jų saugumą, turėti sisteminių programinių priemonių administravimo ir priežiūros patirties, mokėti administruoti ir prižiūrėti duomenų bazes, 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, *nix*, *Oracle, SQL*) administravimo ir priežiūros patirties.
34. VEPIS naudotojai privalo turėti atitinkamą kvalifikaciją, būti apmokyti dirbti su VEPIS programine įranga, supažindinti saugaus darbo su duomenimis principais, turėti patirties dirbant su *Windows* operacinėmis sistemomis, taikomosiomis programomis, būti pasirašę pasižadėjimą saugoti asmens duomenų ir kitą VEPIS elektroninę informacijos paslaptį.

V. SKYRIUS

INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

35. Tvarkyti VEPIS elektroninę informaciją gali tik VEPIS naudotojai, susipažinę su Saugos nuostatais, VEPIS saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, bei atsakomybe už saugos dokumentų nuostatų pažeidimus, ir raštu sutikę laikytis saugos dokumentuose nustatytų reikalavimų. Pakartotinis supažindinimas yra vykdomas pasikeitus minėtiems dokumentams ir teisės aktams.
36. Už VEPIS naudotojų supažindinimą su šiais Saugos nuostatais ir VEPIS saugos politiką įgyvendinančiais dokumentais yra atsakingas VEPIS saugos įgaliotinis.
37. VEPIS naudotojams turi būti nuolat rengiami duomenų saugos mokymai, įvairiais būdais primenama apie saugos problematiką (pvz., priminimai elektroniniu būdu, teminių seminarų rengimas ir pan.). Už saugumo problemų priminimą, mokymų organizavimą atsako VEPIS saugos įgaliotinis. Už saugumo problemų priminimą, mokymų planavimą ir organizavimą atsako WEPIS saugos įgaliotinis.

VI. SKYRIUS

BAIGIAMOSIOS NUOSTATOS

38. Saugos nuostatai ne rečiau kaip kartą per metus arba įvykus esminiams pokyčiams turi būti peržiūrimi.
39. VEPIS administratoriai, VEPIS saugos įgaliotinis, VEPIS naudotojai, VEPIS duomenų teikėjai, VEPIS aptarnavimo paslaugų teikėjai pažeidę VEPIS elektroninės informacijos saugą reglamentuojančių dokumentų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

SUDERINTA
Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos
2018 m. balandžio 24 d. raštu Nr.(4.2) 6K-233 „Dėl duomenų saugos dokumentų suderinimo“