Projektas

LIETUVOS RESPUBLIKOS VYRIAUSYBĖ

NUTARIMAS DĖL VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ, KURIE TURI BŪTI PRIEINAMI KARO PADĖTIES, NEPAPRASTOSIOS PADĖTIES, EKSTREMALIŲJŲ SITUACIJŲ AR KITAIS KRIZIŲ ATVEJAIS, KOPIJŲ LAIKYMO EUROPOS SĄJUNGOS VALSTYBĖSE NARĖSE, EUROPOS EKONOMINĖS ERDVĖS VALSTYBĖSE IR (ARBA) ŠIAURĖS ATLANTO SUTARTIES ORGANIZACIJOS (NATO) VALSTYBĖSE NARĖSE ESANČIUOSE DUOMENŲ CENTRUOSE, IR ŠIŲ IŠTEKLIŲ VEIKLOS ATKŪRIMO IŠ KOPIJŲ TVARKOS APRAŠO PATVIRTINIMO

2022 m. d. Nr.
Vilnius

Vadovaudamasi Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 43^3 straipsnio 2 ir 3 dalimis, Lietuvos Respublikos Vyriausybė n u t a r i a:

1. Patvirtinti Valstybės informacinių išteklių, kurie turi būti prieinami karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais, kopijų laikymo Europos Sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (arba) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esančiuose duomenų centruose, ir šių išteklių veiklos atkūrimo iš kopijų tvarkos aprašą (pridedama).

2. Įgalioti Informacinės visuomenės plėtros komitetą centralizuotai sudaryti:

2.1. viešojo pirkimo–pardavimo sutartis dėl valstybės institucijų ir valstybės įstaigų, finansuojamų iš Lietuvos Respublikos valstybės biudžeto, valdomų valstybės informacinių išteklių, kurie turi būti prieinami karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais, kopijų laikymo Europos Sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (arba) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esančiuose duomenų centruose;

2.2. preliminariąsias viešojo pirkimo–pardavimo sutartis dėl valstybės institucijų, valstybės įstaigų, valstybės įmonių ar viešųjų įstaigų, finansuojamų iš kitų, nei nurodyta šio nutarimo 2.1 papunktyje, finansavimo šaltinių, valdomų valstybės informacinių išteklių, kurie turi būti prieinami karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais, kopijų laikymo Europos Sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (arba) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esančiuose duomenų centruose.

Ministras Pirmininkas

Ekonomikos ir inovacijų ministras

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2022 m. d. nutarimu Nr.

VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ, KURIE TURI BŪTI PRIEINAMI KARO PADĖTIES, NEPAPRASTOSIOS PADĖTIES, EKSTREMALIŲJŲ SITUACIJŲ AR KITAIS KRIZIŲ ATVEJAIS, KOPIJŲ LAIKYMO EUROPOS SĄJUNGOS VALSTYBĖSE NARĖSE, EUROPOS EKONOMINĖS ERDVĖS VALSTYBĖSE IR (ARBA) ŠIAURĖS ATLANTO SUTARTIES ORGANIZACIJOS (NATO) VALSTYBĖSE NARĖSE ESANČIUOSE DUOMENŲ CENTRUOSE, IR ŠIŲ IŠTEKLIŲ VEIKLOS ATKŪRIMO IŠ KOPIJŲ TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybės informacinių išteklių, kurie turi būti prieinami karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais, kopijų laikymo Europos Sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (arba) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esančiuose duomenų centruose, ir šių išteklių veiklos atkūrimo iš kopijų tvarkos aprašas (toliau – Aprašas) nustato Lietuvos Respublikos Vyriausybės įgaliotos institucijos ir į Vyriausybės nutarimu patvirtintą sąrašą įtrauktų registrų ir valstybės informacinių sistemų (toliau – VII) valdytojų ir VII tvarkytojų veiksmus, siekiant užtikrinti, kad VII būtų prieinami karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais.

2. Apraše vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos karo padėties įstatyme, Lietuvos Respublikos nepaprastosios padėties įstatyme, Lietuvos Respublikos civilinės saugos įstatyme, Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatyme, Lietuvos Respublikos viešųjų pirkimų įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių apraše, patvirtintuose 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“, vartojamas sąvokas.

3. VII atsarginė kopija, kurią sudaro VII duomenys ir (ar) informacija bei šiuos duomenis ir (ar) informaciją apdorojančios informacinių technologijų priemonės, privalo būti

laikoma ne Lietuvos Respublikoje esančiuose duomenų centruose, bet Europos Sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (arba) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esančiuose duomenų centruose (toliau – užsienio teritorijose esantys duomenų centrai). Rekomenduojama, kad užsienio teritorijose esantys duomenų centrai būtų įrengti Europos Sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (arba) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse, kurios nesiriboja su valstybėmis, įtrauktomis į Valstybių ar teritorijų, kurių tiekėjai, jų subtiekėjai, ūkio subjektai, kurių pajėgumais yra remiamasi, gamintojai, techninės ar programinės įrangos priežiūrą ir palaikymą vykdantys asmenys ar juos kontroliuojantys asmenys nelaikomi patikimais, sąrašą, patvirtintą Lietuvos Respublikos Vyriausybės 2022 m. kovo 30 d. nutarimu Nr. 280 „Dėl Lietuvos Respublikos viešųjų pirkimų įstatymo 92 straipsnio 13, 14 ir 15 dalių nuostatų įgyvendinimo“ (toliau – Nepatikimų valstybių sąrašas).

II SKYRIUS
SUTARČIŲ DĖL VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ, KURIE TURI BŪTI PRIEINAMI KARO PADĖTIES, NEPAPRASTOSIOS PADĖTIES, EKSTREMALIŲJŲ SITUACIJŲ AR KITAIS KRIZIŲ ATVEJAIS, KOPIJŲ LAIKYMO EUROPOS SĄJUNGOS VALSTYBĖSE NARĖSE, EUROPOS EKONOMINĖS ERDVĖS VALSTYBĖSE IR (ARBA) ŠIAURĖS ATLANTO SUTARTIES ORGANIZACIJOS (NATO) VALSTYBĖSE NARĖSE ESANČIUOSE DUOMENŲ CENTRUOSE SUDARYMAS

4. VII atsarginės kopijos laikymui užsienio teritorijose esančiuose duomenų centruose reikalingos paslaugos (toliau – Paslaugos) perkamos Viešųjų pirkimų įstatymo nustatyta tvarka, tikrinant perkančiųjų organizacijų, veikiančių srityse, kurios laikomos nacionaliniam saugumui užtikrinti strategiškai svarbių ūkio sektorių dalimi, ar valdančių ypatingos svarbos informacinę infrastruktūrą, pirkimus, kurių pagrindu susidarytų aplinkybės, nurodytos Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo 13 straipsnio 4 dalies 1 punkte (susijusios su sandorio šalies prieiga prie duomenų), o perkančiosioms organizacijoms, veikiančioms gynybos srityje, valdančioms ypatingos svarbos informacinę infrastruktūrą, veikiančioms srityse, kurios laikomos nacionaliniam saugumui užtikrinti strategiškai svarbių ūkio sektorių dalimi, ar įrašytoms į Saugiojo valstybinio duomenų perdavimo tinklo naudotojų sąrašą, patvirtintą Lietuvos Respublikos Vyriausybės 2018 m. sausio 3 d. nutarimu Nr. 27 „Dėl Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo įgyvendinimo saugiojo valstybinio duomenų perdavimo tinklo ir valstybinių duomenų centrų valdymo srityse“, atliekančioms paslaugų pirkimus, kurių objektų Bendrojo viešųjų pirkimų žodyno kodai nurodomi Viešojo pirkimo objektų, nurodytų Lietuvos Respublikos viešųjų pirkimų įstatymo 37 straipsnio 9 dalyje ir 47 straipsnio 9 dalyje, Bendrojo viešųjų pirkimų žodyno kodų sąraše, patvirtintame Lietuvos Respublikos Vyriausybės 2022 m. kovo 30 d. nutarimu Nr. 280 „Dėl

Lietuvos Respublikos viešųjų pirkimų įstatymo 92 straipsnio 13, 14 ir 15 dalių nuostatų įgyvendinimo“, nebūtų sudarytos sąlygos šių paslaugų įsigyti iš tiekėjų, registruotų (jeigu gamintojas ar jį kontroliuojantis asmuo yra fizinis asmuo – nuolat gyvenantis Nepatikimų valstybių sąraše nurodytose valstybėse ar teritorijose arba turintys šių valstybių pilietybę) valstybėse, kurios įtrauktos į Nepatikimų valstybių sąrašą.

5. Sutartys dėl Paslaugų (toliau – Sutartys) sudaromos tarp Paslaugų gavėjų, nurodytų Aprašo 6 punkte, ir Paslaugų teikėjų.

6. Paslaugų gavėjais laikomi:

6.1. Vyriausybės įgaliota institucija – tuo atveju, kai VII valdytojai yra valstybės institucijos ar valstybės įstaigos, finansuojamos iš valstybės biudžeto. Šiuo atveju Vyriausybės įgaliota institucija Sutartis su Paslaugų teikėjais sudaro centralizuotai;

6.2. VII valdytojas – tais atvejais, kai VII valdytojai yra valstybės institucijos, valstybės įstaigos, valstybės įmonės ar viešosios įstaigos, finansuojamos iš kitų, nei nurodyta Aprašo 6.1 papunktyje, finansavimo šaltinių.

7. Tuo atveju, kai Sutartis su Paslaugų teikėjais centralizuotai sudaro Vyriausybės įgaliota institucija, VII valdytojas turi pasirašyti su Vyriausybės įgaliota institucija sutartį dėl informacinių technologijų paslaugų teikimo ir pateikti jai užsakymą dėl VII atsarginių kopijų saugojimo užsienio teritorijose esančiuose duomenų centruose (toliau – Užsakymas).

8. Informacinių technologijų paslaugų teikimo sutartis sudaroma ir Užsakymas pateikiamas ekonomikos ir inovacijų ministro tvirtinamo informacinių technologijų paslaugų teikimo sutarčių standartinių sąlygų aprašo nustatyta tvarka.

9. Į Sutartis, be Viešųjų pirkimų įstatyme nustatytų reikalavimų, turi būti įtrauktos nuostatos dėl:

9.1. Paslaugų gavėjo ir Paslaugų teikėjo atsakomybės už kibernetinį saugumą ir Paslaugų gavėjo ir Paslaugų teikėjo atstovų, atsakingų už kibernetinį saugumą, kontaktinės informacijos (vardas, pavardė, telefono numeris, elektroninio pašto adresas);

9.2. duomenų ir (ar) informacijos ar Paslaugų vientisumo, prieinamumo ir konfidencialumo užtikrinimo reikalavimų;

9.3. Paslaugų kontrolės ir auditavimo, susijusio su kibernetinio saugumo užtikrinimu, reikalavimų;

9.4. Paslaugų perdavimo subteikėjams reikalavimų;

9.5. licencijavimo, intelektinės nuosavybės užtikrinimo reikalavimų;

9.6. duomenų ir (ar) informacijos kopijos apimties;

9.7. regionų ar prieinamumo zonų, kuriose duomenų ir (ar) informacija bus saugoma, nustatant reikalavimus Paslaugų teikėjui pranešti apie Paslaugų teikimo regiono ar prieinamumo zonos keitimą;

9.8. prieigos prie visų įvykių ir audito įrašų, susijusių su Paslaugos gavėju ar jam teikiamomis Paslaugomis, reikalavimų;

9.9. Paslaugų ar duomenų ir (ar) informacijos perkėlimo ar sunaikinimo reikalavimų;

9.10. Paslaugų teikimo nutraukimo reikalavimų – turi būti nustatytas ne mažesnis kaip vieno mėnesio laikotarpis Paslaugų teikėjui pranešti apie Paslaugų teikimo nutraukimą;

9.11. prieigos prie duomenų ir (ar) informacijos suteikimo ir valdymo reikalavimų – turi būti nustatyta pareiga Paslaugų teikėjui nedelsiant, bet ne vėliau kaip per vieną valandą nuo atsitiktinės ar neteisėtos prieigos prie duomenų ir (ar) informacijos, jos sunaikinimo, pakeitimo, sugadinimo ar kitokio neteisėto tvarkymo ar prieigos fakto, apie tai pranešti Paslaugos gavėjui;

9.12. abipusio dalijimosi informacija apie kibernetines grėsmes ir pažeidžiamumą reikalavimų;

9.13. Paslaugų teikėjo techninės įrangos, programinės įrangos, Paslaugų testavimo reikalavimų;

9.14. Paslaugų teikėjo veiklos tęstinumo ir nenumatytų atvejų valdymo reikalavimų;

9.15. abipusio pranešimo apie sutrikimus ir kibernetinius incidentus tvarkos ir sutrikimų, kibernetinių incidentų valdymo tvarkos;

9.16. Paslaugų teikėjo prievolės, siekiant užtikrinti atitiktį 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“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas), 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“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas), ir krašto apsaugos ministro tvirtinamo techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo (toliau – Elektroninės informacijos saugos reikalavimų aprašas) reikalavimams, taip pat kitiems valstybės informacinių išteklių saugą ir (ar) kibernetinį saugumą reglamentuojantiems teisės aktams.

10. Prieš sudarydamas Sutartį su Paslaugų teikėju, Paslaugų gavėjas turi įvertinti savo galimybes ir riziką:

10.1. įvykdyti asmens duomenų apsaugą, elektroninės informacijos saugą ir (ar) kibernetinį saugumą reglamentuojančių teisės aktų, sutartinių įsipareigojimų, veiklos standartų ir vidaus teisės aktų reikalavimus;

10.2. išlaikyti nuosavybės teises į Paslaugų teikėjo saugomą duomenų ir (ar) informacijos kopiją;

10.3. užtikrinti VII veiklos tęstinumą ir pajėgumą atkurti VII veiklą tuo atveju, jei Paslaugų teikėjas prarastų jo saugomą duomenų ir (ar) informacijos kopiją arba iš šios kopijos nebūtų galimybės atkurti VII veiklą;

10.4. imtis priemonių, jei Paslaugų teikėjo saugomos duomenų ir (ar) informacijos kopijos būtų atsitiktiniai ar neteisėtai atskleistos;

10.5. valdyti prieigą prie Paslaugų teikėjui perduotų VII duomenų ir (ar) informacijos kopijų ir užtikrinti Paslaugų teikėjui perduotų VII duomenų ir (ar) informacijos kopijų konfidencialumą, vientisumą ir prieinamumą;

10.6. gauti iš Paslaugų teikėjo informaciją apie privatumo ir kibernetinio saugumo reikalavimų pažeidimus;

10.7. taikyti Paslaugų teikėjui užsienio valstybės, kurioje veikia Paslaugų teikėjas, įstatymus, kurie gali turėti neigiamos įtakos perduotoms VII duomenų ir (ar) informacijos kopijoms.

11. Sutarties su Paslaugų teikėju galimybių ir rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kurią tvirtina Paslaugų gavėjas. Paslaugų gavėjas, atsižvelgdamas į rizikos įvertinimo ataskaitą, prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

12. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas Paslaugų gavėjas ne vėliau kaip per 5 darbo dienas šių dokumentų parengimo ar atnaujinimo dienos pateikia Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos.

III SKYRIUS
VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ, KURIE TURI BŪTI PRIEINAMI KARO PADĖTIES, NEPAPRASTOSIOS PADĖTIES, EKSTREMALIŲJŲ SITUACIJŲ AR KITAIS KRIZIŲ ATVEJAIS, KOPIJŲ PARENGIMO IR PERDAVIMO Į EUROPOS SĄJUNGOS VALSTYBĖSE NARĖSE, EUROPOS EKONOMINĖS ERDVĖS VALSTYBĖSE IR (ARBA) ŠIAURĖS ATLANTO SUTARTIES ORGANIZACIJOS (NATO) VALSTYBĖSE NARĖSE ESANČIUS DUOMENŲ CENTRUS TVARKA

13. VII atsarginės kopijos parengimą ir perdavimą į užsienio teritorijose esančius duomenų centrus organizuoja VII valdytojai, vadovaudamiesi Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše ir Elektroninės informacijos saugos reikalavimų apraše nustatytais reikalavimais.

14. VII atsarginės kopijos parengimą ir perdavimą į užsienio teritorijose esančius duomenų centrus vykdo Vyriausybės įgaliota institucija (Aprašo 6.1 papunktyje nurodytu atveju, kai yra pateiktas Užsakymas) arba VII valdytojas ar jo įgaliotas VII tvarkytojas (Aprašo 6.2 papunktyje nurodytu atveju).

15. Už tai, kad VII atsarginė kopija būtų laiku parengta ir perduota į užsienio teritorijose esančius duomenų centrus, atsako subjektas, kuris rengia VII atsarginę kopiją ir perduoda ją į užsienio teritorijose esančius duomenų centrus.

16. VII atsarginė kopija parengiama ir į užsienio teritorijose esančius duomenų centrus perduodama tokiu dažnumu, kaip nustatyta VII valdytojo patvirtintame VII veiklos tęstinumo valdymo plane, kituose VII valdytojo arba jo įgalioto VII tvarkytojo tvirtinamuose VII atsarginių kopijų darymą ir VII veiklos atkūrimą iš VII atsarginių kopijų reglamentuojančiuose tvarkos aprašuose.

17. Aprašo 16 punkte nustatytu dažnumu darant VII atsargines kopijas, VII duomenų ir (ar) informacijos pakeitimų praradimas nuo VII duomenų ir (ar) informacijos kopijos padarymo ir patalpinimo užsienio teritorijose esančiame duomenų centre momento yra laikomas priimtinu.

18. Už VII atsarginių kopijų, laikomų užsienio teritorijose esančiuose duomenų centruose, asmens duomenų apsaugą, bendrųjų elektroninės informacijos saugos ir (ar) kibernetinio saugumo reikalavimų įgyvendinimą bei apsaugą nuo neteisėtos prieigos ir neteisėto atkūrimo nuo jų perkėlimo į užsienio teritorijose esančius duomenų centrus momento atsako subjektas, kuris vykdo VII atsarginės kopijos parengimą ir perdavimą į užsienio teritorijose esančius duomenų centrus.

19. VII atsarginė kopija parengiama ir į užsienio teritorijose esančius duomenų centrus perduodama užšifruota (šifravimo raktai turi būti saugomi atskirai nuo VII atsarginės kopijos) šifruotu duomenų perdavimo kanalu arba turi būti imtasi kitų techninių priemonių, neleidžiančių panaudoti VII atsargines kopijas neteisėtai jas atkurti.

IV SKYRIUS
PARENGIAMŲJŲ VEIKSMŲ DĖL VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ, KURIE TURI BŪTI PRIEINAMI KARO PADĖTIES, NEPAPRASTOSIOS PADĖTIES, EKSTREMALIŲJŲ SITUACIJŲ AR KITAIS KRIZIŲ ATVEJAIS, VEIKLOS ATKŪRIMO REIKALAVIMAI

20. Vyriausybės įgaliota institucija, gavusi Užsakymą, sukuria VII atsarginėms kopijoms saugoti reikalingą informacinių technologijų infrastruktūrą užsienio teritorijose esančiuose duomenų centruose.

21. Tuo atveju, kai Sutartis su Paslaugų teikėjais centralizuotai sudaro Vyriausybės įgaliota institucija, VII valdytojas ne vėliau kaip per 6 mėnesius nuo Užsakymo pateikimo dienos turi Vyriausybės įgaliotai institucijai pateikti:

21.1. VII architektūros aprašymą bei nurodyti šių VII ryšius su kitais registrais ar valstybės informacinėmis sistemomis ir pažymėti, kurie VII ryšiai su kitais registrais ir valstybės informacinėmis sistemomis yra būtini, siekiant atkurti VII veiklą karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitų krizių atvejais;

21.2. išsamias instrukcijas dėl VII veiklos iš VII atsarginės kopijos, parengtos ir perduotos į užsienio teritorijose esančius duomenų centrus, atkūrimo (įskaitant siektiną atkūrimo terminą, atkūrimo momentą ir atkūrimo kriterijus, kuriais vadovaujantis galima nustatyti, kada VII veikla sėkmingai atkurta) karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitų krizių atvejais;

21.3. informaciją apie VII atsarginės kopijos parengimui ir perdavimui į užsienio teritorijose esančius duomenų centrus bei VII veiklos iš VII atsarginės kopijos atkūrimui taikytinus asmens duomenų apsaugos, bendruosius elektroninės informacijos saugos ir (ar) kibernetinio saugumo reikalavimus.

22. VII valdytojas arba jo pavedimu VII tvarkytojas privalo parengti ar atnaujinti VII veiklos tęstinumo valdymo planus, kitus saugos politiką įgyvendinančius ir VII veiklos tęstinumo užtikrinimą reglamentuojančius dokumentus dėl pasirengimo karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitiems krizių atvejams ir juose nurodyti:

22.1. darbo procedūras, kurias atliks tol, kol bus atkurta VII veikla;

22.2. VII veiklos iš VII atsarginės kopijos, perduotos į užsienio teritorijose esančius duomenų centrus, atkūrimo procedūras;

22.3. VII veiklos iš VII atsarginės kopijos, perduotos į užsienio teritorijose esančius duomenų centrus, atkūrimo procedūras ir VII veiklos išbandymo instrukcijas ir pateikti informaciją apie siektiną VII veiklos atkūrimo laiką, atkūrimo momentą ir atkūrimo kriterijus, kuriais vadovaujantis galima nustatyti, kada VII veikla laikoma atkurta;

22.4. VII administratorių slaptažodžių saugojimo, keitimo ir panaudojimo procedūras ir instrukcijas;

22.5. VII valdytojų, VII tvarkytojų ir Vyriausybės įgaliotos institucijos (Aprašo 6.1 papunktyje nurodytu atveju) atstovų tapatybės nustatymo ir prieigos prie VII valdymo procedūras ir instrukcijas;

22.6. taikytinas asmens duomenų apsaugos, bendrosios elektroninės informacijos saugos ir (ar) kibernetinio saugumo kontrolės priemones tol, kol bus atkurta VII veikla;

22.7. VII veiklos atkūrimo koordinavimo grupės sudėtį, kuri karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais būtų atsakinga už VII veiklos atkūrimą ir kiekvienos VII veiklos atkūrimo procedūros atlikimą ir instrukcijos vykdymą. Tuo atveju, kai Sutartis su Paslaugų teikėjais centralizuotai sudaro Vyriausybės

įgaliota institucija, į VII veiklos atkūrimo koordinavimo grupės sudėtį turi būti įtraukti Vyriausybės įgaliotos institucijos atstovai.

23. Aprašo 22 punkte nurodyti dokumentai turi būti parengti ar atnaujinti ne vėliau kaip per 6 mėnesius nuo Užsakymo pateikimo Vyriausybės įgaliotai institucijai (Aprašo 6.1 papunktyje nurodytu atveju) arba Sutarties sudarymo dienos (Aprašo 6.2 papunktyje nurodytu atveju). Šie dokumentai rengiami vadovaujantis Saugos dokumentų turinio 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“ nuostatomis.

24. Parengęs ar atnaujinęs Aprašo 22 punkte nurodytus dokumentus, apie tai VII valdytojas arba jo įgaliotas VII tvarkytojas privalo informuoti Nacionalinį kibernetinio saugumo centrą prie Krašto apsaugos ministerijos ir Vyriausybės įgaliotą instituciją (Aprašo 6.1 papunktyje nustatytu atveju) ne vėliau kaip per 5 darbo dienas šių dokumentų parengimo ar atnaujinimo dienos.

V SKYRIUS
VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ, KURIE TURI BŪTI PRIEINAMI KARO PADĖTIES, NEPAPRASTOSIOS PADĖTIES, EKSTREMALIŲJŲ SITUACIJŲ AR KITAIS KRIZIŲ ATVEJAIS, VEIKLOS ATKŪRIMO TVARKA

25. Karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais Lietuvos teritorijoje praradus prieigą prie VII ar sutrikus jų veiklai ir nesant galimybės jos atkurti, turi būti inicijuojamas šių VII atkūrimas iš VII atsarginės kopijos, laikomos užsienio teritorijose esančiuose duomenų centruose.

26. Aprašo 25 punkte nurodytu atveju VII valdytojas ar jo įgaliotas VII tvarkytojas apie poreikį atkurti VII veiklą iš VII atsarginės kopijos praneša karo padėtį, nepaprastąją padėtį, ekstremaliąją situaciją ar krizę valdantiems subjektams, kurie priima sprendimą dėl VII veiklos atkūrimo terminų ir prioritetų, vadovaudamiesi atitinkamos situacijos valdymą reguliuojančių teisės aktų reikalavimais.

27. VII veiklą iš VII atsarginės kopijos, perduotos į užsienio teritorijose esančius duomenų centrus, atkuria subjektai, kurie organizavo ir vykdė VII atsarginės kopijos parengimą ir perdavimą į užsienio teritorijose esančius duomenų centrus, VII veiklos tęstinumo valdymo plane nustatyta tvarka.

28. Karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar krizių atvejais Lietuvos teritorijoje praradus prieigą prie VII ar sutrikus jų veiklai, VII veiklos atkūrimo

koordinavimo grupės nariai pagal kompetenciją imasi veiksmų siekdami, kad, vadovaujantis karo padėtį, nepaprastąją padėtį, ekstremaliąją situaciją ar krizę valdančių subjektų sprendimu, VII veikla būtų atkurta Lietuvos teritorijoje ar už jos ribų.

VI SKYRIUS
FINANSAVIMO ŠALTINIAI

29. VII atsarginių kopijų parengimas ir perdavimas į užsienio teritorijose esančius duomenų centrus finansuojamas iš:

29.1. Vyriausybės įgaliotai institucijai skirtų valstybės biudžeto asignavimų – Aprašo 6.1 papunktyje nustatytais atvejais;

29.2. VII valdytojui skirtų asignavimų – Aprašo 6.2 papunktyje nustatytais atvejais.

_____