Suvestinė redakcija nuo 2021-07-22

Įsakymas paskelbtas: TAR 2020-08-19, i. k. 2020-17529

LIETUVOS RESPUBLIKOS SUSISIEKIMO MINISTRAS

ĮSAKYMAS
DĖL TRANSPORTO PRIEMONIŲ, LAUKIANČIŲ KIRSTI LIETUVOS RESPUBLIKOS VALSTYBĖS SIENĄ, EILIŲ VALDYMO INFORMACINĖS SISTEMOS NUOSTATŲ IR TRANSPORTO PRIEMONIŲ, LAUKIANČIŲ KIRSTI LIETUVOS RESPUBLIKOS VALSTYBĖS SIENĄ, EILIŲ VALDYMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2020 m. rugpjūčio 19 d. Nr. 3-461
Vilnius

Pakeistas teisės akto pavadinimas:
Nr. 3-361, 2021-07-21, paskelbta TAR 2021-07-21, i. k. 2021-16185

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 30 straipsnio 2 ir 3 dalimis, 31 straipsniu ir 32 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“, 11 punktu ir 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:

1. N u s p r e n d ž i u modernizuoti Pasienio kontrolės punktų informacinę sistemą, įsteigtą Lietuvos Respublikos susisiekimo ministro 2013 m. gruodžio 27 d. įsakymu Nr. 3-653 „Dėl Pasienio kontrolės punktų informacinės sistemos nuostatų ir Pasienio kontrolės punktų informacinės sistemos duomenų saugos nuostatų patvirtinimo“.

2. T v i r t i n u pridedamus:

2.1. Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos nuostatus;

2.2. Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos saugos nuostatus.

3. P a v e d u Pasienio kontrolės punktų direkcijai prie Susisiekimo ministerijos:

3.1. paskirti Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos duomenų valdymo įgaliotinį, saugos įgaliotinį ir administratorių, o jeigu administratoriaus funkcijos Valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka perduotos paslaugos teikėjui, asmenį, kontroliuojantį šio paslaugos teikėjo darbą;

3.2. ne vėliau kaip per 6 mėnesius nuo šio įsakymo įsigaliojimo dienos pateikti Lietuvos Respublikos susisiekimo ministrui tvirtinti Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos saugos politikos įgyvendinamųjų dokumentų projektus;

3.3. patvirtinus Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos nuostatus ir Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos saugos nuostatus, Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos tvarkytojui parengti šios informacinės sistemos techninio aprašymo (specifikacijos) pakeitimo projektą.

4. P r i p a ž į s t u netekusiu galios Lietuvos Respublikos susisiekimo ministro 2013 m. gruodžio 27 d. įsakymą Nr. 3-653 „Dėl Pasienio kontrolės punktų informacinės sistemos nuostatų ir Pasienio kontrolės punktų informacinės sistemos duomenų saugos nuostatų patvirtinimo“ su visais pakeitimais ir papildymais.

Susisiekimo ministras Jaroslav Narkevič

PATVIRTINTA
Lietuvos Respublikos susisiekimo ministro
2020 m. rugpjūčio 19 d. įsakymu Nr. 3-461
(Lietuvos Respublikos susisiekimo ministro
2021 m. liepos 21 d. įsakymo Nr. 3-361
redakcija)

TRANSPORTO PRIEMONIŲ, LAUKIANČIŲ KIRSTI LIETUVOS RESPUBLIKOS VALSTYBĖS SIENĄ, EILIŲ VALDYMO INFORMACINĖS SISTEMOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos nuostatai (toliau – Nuostatai) reglamentuoja Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos (toliau – EVIS) steigimo teisinį pagrindą, tikslą, uždavinius, funkcijas, asmens duomenų tvarkymo tikslą, organizacinę, informacinę ir funkcinę struktūras, duomenų naudojimo, teikimo ir saugos, finansavimo, modernizavimo ir likvidavimo tvarką.

2. Nuostatuose vartojamos sąvokos suprantamos taip, kaip jos yra apibrėžtos 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokio duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas), Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos teisės gauti informaciją iš valstybės ir savivaldybių institucijų ir įstaigų 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).

3. EVIS steigimo teisinis pagrindas – Lietuvos Respublikos transporto veiklos pagrindų įstatymo 13^1 straipsnis.

4. Kuriant ir tvarkant EVIS vadovaujamasi:

4.1. Reglamentu (ES) 2016/679;

4.2. Valstybės informacinių išteklių valdymo įstatymu;

4.3. Transporto veiklos pagrindų įstatymu;

4.4. Lietuvos Respublikos valstybės sienos ir jos apsaugos įstatymu;

4.5. Lietuvos Respublikos kibernetinio saugumo įstatymu;

4.6. Teisės gauti informaciją iš valstybės ir savivaldybių institucijų ir įstaigų įstatymu;

4.7. Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo

patvirtinimo“ (toliau – Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas);

4.8. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu;

4.9. 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“;

4.10. Lietuvos Respublikos Vyriausybės 2005 m. kovo 21 d. nutarimu Nr. 296 „Dėl Pasienio kontrolės punktų direkcijos prie Susisiekimo ministerijos steigimo“;

4.11. Lietuvos Respublikos susisiekimo ministro tvirtinamais Pasienio kontrolės punktų direkcijos prie Susisiekimo ministerijos nuostatais;

4.12. Nuostatais;

4.13. susisiekimo ministro tvirtinamais EVIS duomenų saugos nuostatais (toliau – Saugos nuostatai).

5. Pagrindinis EVIS tikslas – informacinių technologijų priemonėmis formuoti motorinių kelių transporto priemonių (toliau – transporto priemonės), laukiančių kirsti Lietuvos Respublikos valstybės sieną išvykstant iš Lietuvos Respublikos, eiles, užtikrinti sklandų šių transporto priemonių patekimą į pasienio kontrolės punktus (toliau – PKP).

6. Asmens duomenų tvarkymo tikslas – identifikuoti asmenis, kuriems informacinių ir ryšių technologijų (toliau – IRT) kanalais ir priemonėmis nuotoliniu būdu teikiama transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną išvykstant iš Lietuvos Respublikos, išankstinio eilės rezervavimo paslauga (toliau – EVIS elektroninė paslauga), valstybės tarnautojus ir darbuotojus, dirbančius pagal darbo sutartis ir turinčius teisę naudotis EVIS ištekliais numatytoms funkcijoms atlikti, bei juridinių asmenų darbuotojus ar asmenis, kuriems Valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka perduodamos EVIS ir (ar) jos infrastuktūros priežiūros funkcijos, turinčius teisę naudotis EVIS ištekliais sutartiniams įsipareigojimams vykdyti (toliau – EVIS naudotojai), prižiūrėti ir valdyti EVIS procesus, fiksuojant šių asmenų EVIS atliekamus veiksmus, taip pat identifikuoti mokėtojus, jiems atliekant mokėjimus už EVIS elektroninę paslaugą.

7. Pagrindiniai EVIS uždaviniai yra šie:

7.1. automatizuoti transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną išvykstant iš Lietuvos Respublikos, eilių valdymą;

7.2. IRT kanalais ir priemonėmis nuotoliniu būdu teikti EVIS elektroninę paslaugą.

8. Pagrindinės EVIS funkcijos yra šios:

8.1. priimti EVIS elektroninės paslaugos užsakymo duomenis;

8.2. kaupti, apdoroti, sisteminti ir teikti EVIS duomenis;

8.3. formuoti mokėjimo už EVIS elektroninę paslaugą ruošinius ir pateikti juos asmenims, kuriems teikiama EVIS elektroninė paslauga;

8.4. sudaryti transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną išvykstant iš Lietuvos Respublikos, virtualią eilę ir skelbti šios eilės tvarkaraštį;

8.5. vykdyti transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną išvykstant iš Lietuvos Respublikos, eismo valdymą iki įvažiavimo į PKP:

8.5.1. valdyti šviesoforus, pakeliamuosius užtvarus, elektroninius ženklus, taip pat automatiškai valdyti šiuos įrenginius pagal iš anksto suprogramuotą loginį sprendinį;

8.5.2. automatiškai fiksuoti įvažiuojančių į PKP transporto priemonių valstybinio registracijos numerio ženklus (toliau – transporto priemonių valstybiniai numeriai);

8.6. fiksuoti EVIS naudotojų ir asmenų, kurie naudojasi EVIS elektronine paslauga (toliau – EVIS elektroninės paslaugos gavėjai), veiksmus, EVIS įvykius.

II SKYRIUS
ORGANIZACINĖ STRUKTŪRA

9. EVIS valdytoja ir asmens duomenų valdytoja yra Lietuvos Respublikos susisiekimo ministerija (Gedimino pr. 17, 01505 Vilnius) (toliau – EVIS valdytojas).

10. EVIS tvarkytoja yra Pasienio kontrolės punktų direkcija prie Susisiekimo ministerijos (toliau – Direkcija) (Gedimino pr. 26, 01104 Vilnius).

11. EVIS valdytojas vykdo Reglamente (ES) 2016/679 nustatytas duomenų valdytojo teises ir pareigas ir atlieka šias funkcijas:

11.1. tvirtina teisės aktus, susijusius su EVIS veikimu;

11.2. koordinuoja Direkcijos darbą ir užtikrina, kad EVIS būtų tvarkoma vadovaujantis Lietuvos Respublikos įstatymais, Nuostatais;

11.3. organizuoja duomenų saugos užtikrinimą;

11.4. planuoja išteklius, skirtus EVIS kurti, prižiūrėti, tobulinti ir plėtoti;

11.5. tvirtina EVIS kūrimo ir plėtros planus, analizuoja pasiūlymus dėl EVIS veikimo, priima sprendimus dėl EVIS tobulinimo ir modernizavimo ir kontroliuoja jų vykdymą;

11.6. vykdo kitas funkcijas, teises ir pareigas, nustatytas Valstybės informacinių išteklių valdymo įstatyme ir kituose teisės aktuose.

12. Direkcijos funkcijos:

12.1. vykdyti EVIS veikimo, techninės ir programinės įrangos priežiūrą;

12.2. tvarkyti EVIS duomenis ir užtikrinti jų saugą;

12.3. sudaryti duomenų teikimo sutartis;

12.4. užtikrinti EVIS veiklos tęstinumą ir veiklos atkūrimą, šalinti sutrikimus;

12.5. teikti EVIS valdytojui pasiūlymus dėl EVIS veikimo ir tobulinimo, organizuoti EVIS valdytojo priimtų sprendimų dėl EVIS tobulinimo ir modernizavimo įgyvendinimą;

12.6. pagal kompetenciją registruoti EVIS naudotojus, tvarkyti jų duomenis, prieigos teises ir klasifikatorius;

12.7. analizuoti EVIS procesus ir EVIS naudotojų veiksmus;

12.8. kurti duomenų mainų sąsajas su duomenų teikėjais ir vykdyti jų priežiūrą;

12.9. konsultuoti EVIS naudotojus ir EVIS elektroninės paslaugos gavėjus su EVIS veikimu susijusiais klausimais;

12.10. organizuoti EVIS naudotojų mokymus;

12.11. formuoti ir teikti reikiamas ataskaitas ir EVIS duomenų sąrankas;

12.12. nustatyti EVIS elektroninės paslaugos teikimo tvarką ir sąlygas;

12.13. Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka organizuoti pirkimo procedūras ir sudaryti sutartis su juridiniais asmenimis ar asmenimis (asmenų grupėmis), kuriems Valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka perduodamos EVIS ir (ar) jos infrastuktūros priežiūros funkcijos (toliau – EVIS paslaugos teikėjas (-ai);

12.14. vykdyti kitas funkcijas, teises ir pareigas, nustatytas Valstybės informacinių išteklių valdymo įstatyme ir kituose teisės aktuose.

13. Asmens duomenų tvarkytoja yra Direkcija.

14. Direkcija vykdo Reglamente (ES) 2016/679 nustatytas duomenų tvarkytojo teises ir pareigas ir įgyvendina duomenų subjektų teises, numatytas Reglamento (ES) 2016/679 III skyriuje. Reglamento (ES) 2016/679 28 straipsnio 3 dalyje nustatytos duomenų tvarkytojo prievolės duomenų valdytojo atžvilgiu detaliai aptariamos asmens duomenų tvarkymo sutartyje, sudarytoje tarp EVIS valdytojo ir Direkcijos.

15. EVIS paslaugos teikėjas (-ai) yra EVIS tvarkytojas (-ai) ir EVIS duomenų tvarkytojo (-ų) pasitelktas kitas asmens duomenų tvarkytojas (-ai), kuris (-ie):

15.1. Direkcijos pavedimu tvarko asmens duomenis ir vykdo Reglamento (ES) 2016/679 28 straipsnio 3 dalyje nustatytas prievoles. Detalios Reglamento (ES) 2016/679 28 straipsnio 4 dalyje nustatytos sąlygos nurodomos asmens duomenų tvarkymo sutartyje (-yse), sudarytoje (-ose) tarp Direkcijos ir EVIS paslaugos teikėjo (-ų);

15.2. atlieka Valstybės informacinių išteklių valdymo įstatyme valstybės informacinės sistemos tvarkytojui nustatytas funkcijas ir įgyvendina šio įstatymo 34 straipsnio 6 dalies 1–6 ir 12 punktuose nurodytas teises ir pareigas;

15.3. suteikia techninius išteklius EVIS programinei įrangai talpinti;

15.4. vykdo EVIS veikimo, techninės ir programinės įrangos palaikymą ir priežiūrą;

15.5. tvarko EVIS duomenis ir užtikrina jų saugą;

15.6. kuria duomenų mainų sąsajas su duomenų teikėjais ir vykdo jų priežiūrą;

15.7. konsultuoja EVIS elektroninės paslaugos gavėjus su EVIS elektroninės paslaugos teikimu susijusiais klausimais.

16. EVIS duomenų teikėjai yra EVIS elektroninės paslaugos gavėjai.

17. EVIS naudojantys asmenys:

17.1. EVIS elektroninės paslaugos gavėjai;

17.2. muitinės pareigūnai;

17.3. Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos pareigūnai.

18. EVIS elektroninės paslaugos gavėjų teisės ir pareigos:

18.1. kiekvienas EVIS elektroninės paslaugos gavėjas turi teisę kreiptis į EVIS valdytoją ir (ar) Direkciją ir susipažinti su EVIS tvarkomais duomenimis, kurie EVIS elektroninės paslaugos gavėjo prašymu jam gali būti pateikti elektroninių ryšių priemonėmis;

18.2. EVIS elektroninės paslaugos gavėjas turi užtikrinti teikiamų duomenų teisingumą ir išsamumą.

III SKYRIUS
INFORMACINĖ STRUKTŪRA

19. EVIS transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, duomenys:

19.1. transporto priemonės kategorija;

19.2. transporto priemonės markė;

19.3. transporto priemonės modelis;

19.4. transporto priemonės valstybinis registracijos numeris (jeigu transporto priemonę sudaro vilkikas ir priekaba (-os) – vilkiko valstybinis registracijos numeris);

19.5. transporto priemonės judėjimo duomenys (transporto priemonės atvykimo į nurodytą laukimo vietą (toliau – laukimo aikštelė) priešais PKP laikas ir data, įvažiavimo į PKP teritoriją laikas ir data);

19.6. valstybės sienos kirtimo statuso požymiai (vyksta bendros eilės tvarka, turi teisės aktais suteiktą teisę Lietuvos Respublikos valstybės sieną kirsti be eilės).

20. EVIS elektroninės paslaugos gavėjų duomenys:

20.1. prisijungimo duomenys (prisijungimo vardas, slaptažodis);

20.2. fizinio asmens vardas (-ai) ir pavardė (-ės);

20.3. fizinio asmens elektroninio pašto adresas (jeigu asmuo naudojasi el. paštu);

20.4. fizinio asmens telefono ryšio numeris (jeigu asmuo naudojasi telefonu);

20.5. juridinio asmens pavadinimas;

20.6. juridinio asmens kodas;

20.7. pridėtinės vertės mokesčio mokėtojo kodas (jeigu asmuo turi šį kodą);

20.8. juridinio asmens adresas;

20.9. juridinio asmens telefono ryšio numeris;

20.10. juridinio asmens elektroninio pašto adresas;

20.11. teisės aktų nustatyta tvarka suteikto prioriteto kirsti Lietuvos Respublikos valstybės sieną pirmumo tvarka požymis ir pagrindas.

21. PKP duomenys (pavadinimas, adresas, žemėlapis (paveikslėlis).

22. Laukimo aikštelės duomenys (pavadinimas, adresas, žemėlapis (paveikslėlis), kontaktiniai duomenys).

23. Rezervacijos ir virtualios Lietuvos Respublikos valstybės sienos kirtimo eilės duomenys (rezervacijos būsena (rezervuota / nerezervuota / sumokėta / atšaukta / iškviesta / įvažiavęs į PKP), data, laikas, transporto priemonių skaičius, kviečiamų kirsti valstybės sieną transporto priemonių sąrašas, eilės tipas).

24. EVIS elektroninės paslaugos duomenys (EVIS elektroninės paslaugos aprašymas, naudojimosi sąlygos, teisės aktai ir kita, su EVIS elektroninės paslaugos teikimu susijusi informacija).

25. Duomenų apdorojimo procesų rezultatai:

25.1. EVIS naudotojų ir EVIS elektroninės paslaugos gavėjų EVIS atliktų veiksmų duomenys: veiksmo data, laikas, tipas (duomenų įrašymas, koregavimas, naikinimas);

25.2. patekimo į PKP įrenginių (informacinių švieslenčių, pakeliamųjų kelio užtvarų, vaizdo stebėjimo ir įrašymo įrenginių, numerių skenavimo įrenginių ir vietinės pagalbos linijos priemonių) programinės įrangos duomenys ir jų atvaizdavimo parametrai;

25.3. EVIS veiksmų ir veikimo sutrikimų ir kiti techniniai duomenys.

26. Mokėjimo už EVIS elektroninę paslaugą (toliau – mokėjimas) duomenys:

26.1. paslaugos kaina;

26.2. paslaugos užsakymo numeris:

26.3. mokėjimo pavedimo numeris;

26.4. mokėjimo kodas;

26.5. mokėtojo vardas, pavardė ir (ar) pavadinimas;

26.6. mokėjimo paskirtis;

26.7. operacijos įvykdymo data;

26.8. sąskaitos faktūros numeris;

26.9. pavedimo suma;

26.10. valiutos pavadinimas (kodas);

26.11. pinigų gavėjo sąskaitos numeris;

26.12. pinigų gavėjo pavadinimas.

27. Duomenų teikėjų teikiami duomenys – EVIS elektroninės paslaugos gavėjai teikia Nuostatų 19.1–19.4 ir 20.1–20.11 papunkčiuose nurodytus duomenis.

IV SKYRIUS
FUNKCINĖ STRUKTŪRA

28. EVIS funkcinę struktūrą sudaro šie komponentai:

28.1. EVIS portalas, realizuojantis EVIS elektroninės paslaugos gavėjų sąsają;

28.2. EVIS transporto priemonių, kertančių Lietuvos Respublikos valstybės sieną, eilių valdymo modulis, kurį sudaro šie komponentai:

28.2.1. EVIS elektroninės paslaugos teikimo modulis, kurį sudaro:

28.2.1.1. EVIS elektroninės paslaugos gavėjų identifikavimo ir teisių valdymo komponentas; jo pagrindinės funkcijos – EVIS elektroninės paslaugos gavėjų identifikavimas, profilių kūrimas, administravimas, teisių nustatymas;

28.2.1.2. EVIS elektroninės paslaugos užsakymo komponentas; jo pagrindinės funkcijos – duomenų surinkimas ir kaupimas, rezervuojant Lietuvos Respublikos sienos kirtimo datą, laiką ir vietą transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną išvykstant iš Lietuvos Respublikos, eilėje;

28.2.1.3. EVIS elektroninės paslaugos teikimo eigos stebėsenos komponentas; jo pagrindinės funkcijos – EVIS elektroninės paslaugos gavėjų užsakytos paslaugos vykdymo ir suteikimo veiksmų ir paslaugų rezultatų pateikimo registravimas, užsakymo duomenų keitimas;

28.2.1.4. mokėjimo už suteiktą EVIS elektroninę paslaugą komponentas; jo pagrindinė funkcija – realiuoju laiku sekti mokėjimų už EVIS elektroninę paslaugą vykdymą;

28.2.2. EVIS informacijos įvedimo modulis; jo pagrindinė funkcija – sudaryti sąlygas EVIS elektroninės paslaugos gavėjams ir EVIS naudotojams įvesti informaciją;

28.2.3. EVIS duomenų tvarkymo modulis; jo pagrindinės funkcijos – rinkti, kaupti, saugoti, pertvarkyti, apdoroti, archyvuoti ir teikti duomenis, valdyti duomenų bazes ir duomenų analizės įrankius, formuoti ataskaitas;

28.2.4. EVIS administravimo modulis; jo pagrindinės funkcijos – registruoti EVIS naudotojus ir administruoti jų teises, valdyti EVIS veikimo parametrus, registruoti EVIS atliekamus veiksmus, veikimo sutrikimus, formuoti ataskaitas;

28.2.5. patekimo į pasienio kontrolės punktą įrenginių, valdomų EVIS, duomenų tvarkymo modulis; jo pagrindinės funkcijos – rinkti duomenis iš įrenginių ir juos tvarkyti, stebėti įrenginių būklę, registruoti įrenginių gedimus, skelbti transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną išvykstant iš Lietuvos Respublikos, eilės tvarkaraštį, informaciją kintamos informacijos ženkluose ir ją stebėti.

V SKYRIUS
EVIS DUOMENŲ TEIKIMAS IR NAUDOJIMAS, NETIKSLIŲ, NETEISINGŲ, NEIŠSAMIŲ DUOMENŲ IŠTAISYMAS

29. EVIS duomenys, išskyrus asmens duomenis, yra vieši ir teikiami institucijoms, kitiems juridiniams ir fiziniams asmenims (toliau – duomenų gavėjai), jeigu Lietuvos Respublikos įstatymai ir (ar) Europos Sąjungos teisės aktai nenustato kitaip.

30. Viešai skelbiama transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną išvykstant iš Lietuvos Respublikos, eilė ir kita informacija apie transporto priemonių eiles pasienyje, kurios įstatymai ir kiti teisės aktai nedraudžia skelbti viešai. Asmens duomenys viešai neskelbiami.

31. EVIS duomenys, įskaitant asmens duomenis, teikiami pagal Direkcijos ir duomenų gavėjo sudarytą duomenų teikimo sutartį (daugkartinio teikimo atveju) arba duomenų gavėjo prašymą (vienkartinio teikimo atveju). Sutartyje nurodomas EVIS duomenų, įskaitant asmens duomenis, naudojimo tikslas, teikimo ir gavimo teisinis pagrindas, sąlygos, tvarka, teikiamų EVIS duomenų, įskaitant asmens duomenis, apimtis, formatas, gavimo būdas ir teikimo terminai. Prašyme nurodomas EVIS duomenų, įskaitant asmens duomenis, naudojimo tikslas, teikimo ir gavimo teisinis pagrindas, prašomų pateikti EVIS duomenų, įskaitant asmens duomenis, apimtis ir formatas, gavimo būdas.

32. EVIS duomenis, įskaitant asmens duomenis, duomenų gavėjas gali naudoti tik tokiam tikslui, tokios apimties ir tokiu būdu, kokie buvo nurodyti duomenų gavėjo prašyme arba duomenų teikimo sutartyje.

33. Asmens duomenys teikiami vadovaujantis Reglamentu (ES) 2016/679.

34. EVIS duomenys gali būti:

34.1. pateikiami peržiūrėti leidžiamosios kreipties būdu internetu ar kitais elektroninių ryšių tinklais;

34.2. perduodami automatiniu būdu elektroninių ryšių tinklais;

34.3. teikiami raštu, žodžiu ir (arba) elektroninių ryšių priemonėmis.

35. Direkcija teikia EVIS duomenų išrašus, pagal EVIS duomenis parengtas ataskaitas, apibendrintą, susistemintą ar kitaip apdorotą informaciją, duomenų teikėjų pateiktus dokumentus ir (arba) jų kopijas. Duomenų gavėjams teikiami tokio turinio ir tokio formato EVIS duomenys, kurie Direkcijos jau naudojami ir kurių nereikia papildomai apdoroti.

36. Jeigu parengtinis perduodamų EVIS duomenų turinys ar formatas neatitinka prašančiojo registro ar valstybės informacinės sistemos tvarkytojo poreikių arba prašantysis registro ar valstybės informacinės sistemos tvarkytojas neturi techninių galimybių reikiamai apdoroti gautų EVIS duomenų, jeigu dėl sąsajų tarp registro ir (arba) informacinės sistemos nebuvimo nėra galimybės perduoti reikalingų duomenų, Direkcija Vyriausybės nustatyta tvarka sukuria priemones, reikalingas prašomam EVIS duomenų formatui ar turiniui parengti ir (arba) apdoroti. Šių priemonių sukūrimo sąnaudų tinkamumą ir pagrįstumą vertina Vyriausybės įgaliota institucija ir šios priemonės finansuojamos iš valstybės biudžeto lėšų Vyriausybės nustatyta tvarka.

37. EVIS duomenys teikiami neatlygintinai.

38. EVIS duomenys, įskaitant asmens duomenis, Europos Sąjungos valstybių narių ir (arba) Europos ekonominės erdvės valstybių, trečiųjų šalių fiziniams ir juridiniams asmenims, juridinio

asmens statuso neturintiems subjektams, jų filialams ir atstovybėms teikiami vadovaujantis Reglamentu (ES) 2016/679 ir Valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka.

39. EVIS duomenų teikimas gali būti apribotas Valstybės informacinių išteklių valdymo įstatymo 27 straipsnio 7 dalyje numatytais atvejais.

40. Kai atsisakoma teikti EVIS duomenis, asmeniui, pateikusiam prašymą gauti EVIS duomenis, raštu arba elektroninių ryšių priemonėmis pranešama apie priimtą motyvuotą sprendimą atsisakyti tenkinti jo prašymą ir suteikiama informacija apie tokio sprendimo apskundimo tvarką.

41. EVIS duomenų gavėjai, EVIS duomenų teikėjai ir kiti asmenys, pastebėję netikslumų, turi teisę reikalauti EVIS valdytojo ir (arba) Direkcijos ištaisyti netikslius duomenis, ištrinti neteisingus duomenis, papildyti neišsamius duomenis ar apriboti EVIS duomenų tvarkymą, apie tai raštu pranešdami EVIS valdytojui ir (arba) Direkcijai. Direkcija, gavusi reikalavimą dėl netikslių, neteisingų, neišsamių duomenų (toliau – netikslūs duomenys) tvarkymo, per 5 darbo dienas nuo informacijos gavimo (motyvuotu Direkcijos vadovo sprendimu terminas gali būti pratęstas iki 30 darbo dienų) patikrina EVIS duomenų tikslumą ir, jeigu reikia, ištaiso netikslius duomenis. Pranešimas apie netikslių duomenų ištaisymą arba apie motyvuotą atsisakymą tai padaryti nedelsiant (ne vėliau kaip per vieną darbo dieną) siunčiamas asmeniui, pranešusiam apie netikslius duomenis, paštu ir (ar) elektroninių ryšių priemonėmis. Ištaisiusi netikslius duomenis, Direkcija per vieną darbo dieną nuo jų ištaisymo apie tai praneša EVIS duomenų gavėjams, kuriems perduoti netikslūs duomenys.

VI SKYRIUS
EVIS DUOMENŲ SAUGA

42. EVIS duomenų saugą nustato EVIS valdytojo patvirtinti Saugos nuostatai ir saugos politikos įgyvendinamieji dokumentai, kurie rengiami, derinami ir tvirtinami Bendrųjų elektroninės informacijos saugos reikalavimų apraše nustatyta tvarka.

43. Už EVIS duomenų ir elektroninės informacijos saugą pagal kompetenciją Lietuvos Respublikos įstatymų nustatyta tvarka atsako EVIS valdytojas ir EVIS tvarkytojai. EVIS valdytojas ir EVIS tvarkytojai atsako už duomenų tvarkymo teisėtumą ir pagal kompetenciją privalo įgyvendinti tinkamas organizacines ir technines priemones, skirtas EVIS esantiems duomenims apsaugoti nuo netyčinio ar neteisėto sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų. Minėtos priemonės turi užtikrinti tokio lygio saugumą, kuris atitiktų saugotinų EVIS duomenų pobūdį, aprėptį, kontekstą ir tikslus, taip pat EVIS duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus asmenų teisėms ir laisvėms ir jų tvarkymo riziką.

44. Asmenys, tvarkantys asmens duomenis, įpareigojami saugoti asmens duomenų paslaptį ir už neteisėtą asmens duomenų atskleidimą atsako Lietuvos Respublikos įstatymų nustatyta tvarka. Ši atsakomybė išlieka ir jiems pasitraukus iš valstybės tarnybos, perėjus dirbti į kitas pareigas, pasibaigus jų darbo, sutartiniams ar kitiems santykiams.

45. EVIS duomenys, įskaitant asmens duomenis, duomenų bazėje saugomi 12 mėnesių nuo paskutinio pakeitimo (papildymo). Praėjus šiam laikui, duomenys sunaikinami. Už duomenų sunaikinimą atsakinga Direkcija.

46. EVIS tvarkomų duomenų saugumas užtikrinamas vadovaujantis:

46.1. Reglamentu (ES) 2016/679;

46.2. Valstybės informacinių išteklių valdymo įstatymu;

46.3. Kibernetinio saugumo įstatymu;

46.4. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu;

46.5. Saugos dokumentų turinio gairių aprašu, patvirtintu 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“;

46.6. Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašu, patvirtintu 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“;

46.7. 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“;

46.8. 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“;

46.9. Lietuvos standartais LST ISO/IEC 27001, ISO/IEC 27002 ir kitais Lietuvos ir tarptautiniais „Informacinės technologijos. Saugumo metodai“ grupės standartais, apibūdinančiais saugų informacinės sistemos duomenų tvarkymą;

46.10. Nuostatais;

46.11. Saugos nuostatais.

VII SKYRIUS
EVIS FINANSAVIMAS

47. EVIS kūrimas, tvarkymas ir priežiūra finansuojami iš Lietuvos Respublikos valstybės biudžeto.

VIII SKYRIUS
EVIS MODERNIZAVIMAS IR LIKVIDAVIMAS

48. EVIS modernizuojama ir likviduojama Valstybės informacinių išteklių valdymo įstatymo ir Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo nustatyta tvarka.

49. Likviduojamos EVIS duomenys ir dokumentai perduodami kitai informacinei sistemai, kuri steigiama vietoj likviduojamos, arba sunaikinami ar perduodami valstybės archyvams Lietuvos Respublikos dokumentų ir archyvų įstatymo nustatyta tvarka.

IX SKYRIUS
BAIGIAMOSIOS NUOSTATOS

50. Detali duomenų subjekto teisių įgyvendinimo tvarka nustatyta susisiekimo ministro tvirtinamame Duomenų subjektų teisių įgyvendinimo tvarkant asmens duomenis Lietuvos Respublikos susisiekimo ministerijos valdomuose registruose ir valstybės informacinėse sistemose tvarkos apraše.

51. Už Nuostatų nesilaikymą juridiniai ir fiziniai asmenys atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

_____

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2021 m. birželio 30 d. raštu Nr. 1D-3762

SUDERINTA
Lietuvos Respublikos ekonomikos ir inovacijų ministerijos 2021 m. birželio 21 d. raštu Nr. 3-2938

SUDERINTA
Valstybinės duomenų apsaugos inspekcijos
2021 m. birželio 29 d. raštu Nr. 2R-3383
(3.2 Mr)

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2021 m. birželio 29 d. raštu Nr. (4.1E) 6K-518

PATVIRTINTA
Lietuvos Respublikos susisiekimo ministro
2020 m. rugpjūčio 19 d. įsakymu Nr. 3-461
(Lietuvos Respublikos susisiekimo ministro
2021 m. liepos 21 d. įsakymo Nr. 3-361
redakcija)

TRANSPORTO PRIEMONIŲ, LAUKIANČIŲ KIRSTI LIETUVOS RESPUBLIKOS VALSTYBĖS SIENĄ, EILIŲ VALDYMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos (toliau – EVIS) elektroninės informacijos saugos politiką ir kibernetinio saugumo politiką (toliau – saugos politika), kurių tikslas – nustatyti ir įgyvendinti organizacines, technines ir kitas priemones, suteikiančias galimybę saugiai tvarkyti EVIS duomenis ir užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo netyčinio ar neteisėto sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jos.

2. Saugos nuostatuose vartojamos sąvokos suprantamos taip, kaip jos yra apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarime 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“, Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu
Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“, ir Lietuvos Respublikos standartuose LST ISO/IEC 27002 ir LST ISO/IEC 27001.

3. EVIS saugos politiką nustato šie Lietuvos Respublikos susisiekimo ministro patvirtinti teisės aktai (toliau – saugos politikos įgyvendinamieji dokumentai):

3.1. Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės;

3.2. Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos naudotojų administravimo taisyklės;

3.3. Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos veiklos tęstinumo valdymo planas.

4. Saugos nuostatai kartu su saugos politikos įgyvendinamaisiais dokumentais sudaro saugos dokumentus.

5. EVIS elektroninės informacijos saugos ir kibernetinio saugumo (toliau – EVIS elektroninės informacijos sauga) užtikrinimo tikslai – sudaryti sąlygas saugiai automatizuotomis priemonėmis tvarkyti EVIS elektroninę informaciją, užtikrinti EVIS elektroninės informacijos patikimumą, konfidencialumą, prieinamumą, vientisumą ir tinkamą kompiuterinės, programinės ir ryšių įrangos funkcionavimą.

6. EVIS elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

6.1. EVIS elektroninei informacijai tvarkyti naudojamos techninės ir programinės įrangos kontrolė;

6.2. EVIS elektroninės informacijos tvarkymo kontrolė;

6.3. saugaus darbo su EVIS elektronine informacija kontrolė;

6.4. fizinė EVIS elektroninės informacijos tvarkymo priemonių (tarnybinių stočių, informacijos perdavimo įrangos, programinės įrangos) ir patalpų apsauga;

6.5. EVIS veiklos tęstinumas.

7. Saugos nuostatais privalo vadovautis:

7.1. Pasienio kontrolės punktų direkcijos prie Susisiekimo ministerijos (toliau – Direkcija) valstybės tarnautojai ar darbuotojai, dirbantys pagal darbo sutartis, – EVIS saugos įgaliotinis (toliau – saugos įgaliotinis), EVIS administratorius, EVIS duomenų valdymo įgaliotinis (toliau – duomenų valdymo įgaliotinis);

7.2. Direkcijos Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka išrinkto juridinio asmens ar asmenų (asmenų grupės), kuriems Valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka perduotos EVIS ir (ar) jos infrastuktūros priežiūros funkcijos (toliau – EVIS paslaugos teikėjas (-ai), darbuotojai, informacinių sistemų veiklą reglamentuojančių teisės aktų nustatyta tvarka pagal kompetenciją naudojantys ir (ar) tvarkantys EVIS elektroninę informaciją (toliau – EVIS paslaugos teikėjo (-ų) darbuotojai);

7.3. kiti subjektai, kuriems taikomi Saugos nuostatų reikalavimai.

8. EVIS valdytoja yra Lietuvos Respublikos susisiekimo ministerija (Gedimino pr. 17, 01505 Vilnius), EVIS tvarkytojai yra Direkcija (Gedimino pr. 26, 01104 Vilnius) ir EVIS paslaugos teikėjas (-ai).

9. EVIS valdytojo funkcijos ir atsakomybė:

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

9.2. tvirtina EVIS saugos dokumentus, prižiūri ir kontroliuoja, kad EVIS būtų tvarkoma vadovaujantis šiais dokumentais, EVIS nuostatais ir kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą;

9.3. nagrinėja Direkcijos pasiūlymus dėl EVIS elektroninės informacijos saugos tobulinimo ir priima dėl jų sprendimus;

9.4. atsižvelgdamas į rizikos įvertinimo ataskaitą, prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą;

9.5. priima sprendimą dėl EVIS informacinių technologijų saugos atitikties vertinimo atlikimo;

9.6. prireikus tvirtina EVIS informacinių technologijų saugos atitikties vertinimo metu pastebėtų trūkumų šalinimo planą;

9.7. atsako už EVIS pokyčių ir plėtros įgyvendinimą;

9.8. pagal kompetenciją atsako už EVIS elektroninės informacijos saugą;

9.9. paveda Direkcijai paskirti saugos įgaliotinį, duomenų valdymo įgaliotinį, EVIS administratorių;

9.10. vykdo kitas Saugos nuostatų ir kitų teisės aktų, reglamentuojančių saugų elektroninės informacijos tvarkymą, nustatytas funkcijas.

10. Direkcijos funkcijos ir atsakomybė:

10.1. atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir EVIS saugos reikalavimų atitiktį Saugos nuostatams ir saugos politikos įgyvendinamiesiems dokumentams;

10.2. paskiria saugos įgaliotinį, duomenų valdymo įgaliotinį ir EVIS administratorių;

10.3. rengia EVIS saugos dokumentus ir teikia juos tvirtinti EVIS valdytojo vadovui;

10.4. teikia EVIS valdytojui pasiūlymus dėl EVIS plėtros, saugos ir funkcionalumo;

10.5. organizuoja plėtrą ir EVIS pakeitimų įdiegimą;

10.6. rūpinasi EVIS duomenų saugumu, užtikrina tinkamą EVIS administravimą ir nepertraukiamą EVIS veiklą;

10.7. koordinuoja ir kontroliuoja valstybės tarnautojų ar darbuotojų, dirbančių pagal darbo sutartis ir EVIS naudojančių paskirtoms funkcijoms vykdyti bei EVIS paslaugos teikėjo (-ų) darbuotojų veiklą (toliau – EVIS vidiniai naudotojai);

10.8. pagal kompetenciją atsako už EVIS elektroninės informacijos tvarkymo teisėtumą, saugumą ir užtikrina EVIS saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams ir Saugos nuostatams;

10.9. atlieka kitas EVIS valdytojo pavestas, Saugos nuostatuose bei teisės aktuose, reglamentuojančiuose saugų elektroninės informacijos tvarkymą, priskirtas funkcijas.

11. EVIS paslaugos teikėjo (-ų) vadovas (-ai) paskiria administratorių (-ius) (toliau – EVIS paslaugos teikėjo administratorius), jis nurodomas Direkcijos ir EVIS paslaugų teikėjo (-ų) sudarytoje (-ose) sutartyje (-yse).

12. Saugos įgaliotinio (kibernetinio saugumo vadovo) funkcijos ir atsakomybė:

12.1. teikia pasiūlymus Direkcijos vadovui dėl:

12.1.1. EVIS administratoriaus paskyrimo ir reikalavimų EVIS administratoriui nustatymo;

12.1.2. EVIS informacinių technologijų saugos atitikties vertinimo atlikimo 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“, 43 punkte nurodytoje Lietuvos Respublikos krašto apsaugos ministro tvirtinamoje Informacinių technologijų saugos atitikties vertinimo metodikoje nustatyta tvarka;

12.1.3. saugos dokumentų priėmimo, keitimo ar panaikinimo;

12.2. atsako už tinkamą EVIS saugos reikalavimų ir funkcijų vykdymą;

12.3. organizuoja EVIS rizikos įvertinimą, prireikus – neeilinį EVIS rizikos įvertinimą ir EVIS informacinių technologijų saugos atitikties vertinimą;

12.4. informuoja Direkcijos vadovą apie EVIS saugos problemas;

12.5. teikia EVIS administratoriui, EVIS paslaugos teikėjo administratoriui ir EVIS vidiniams naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;

12.6. koordinuoja saugos dokumentų nuostatų pažeidimų ir (ar) elektroninės informacijos saugos ir kibernetinių incidentų (toliau – saugos incidentai) tyrimus;

12.7. bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos sauga, išskyrus atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės;

12.8. užtikrina EVIS saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams;

12.9. pasirašytinai supažindina EVIS administratorių, EVIS paslaugos teikėjo (-ų) administratorių (-ius) ir EVIS vidinius naudotojus su saugos dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, ir atsakomybe už šių dokumentų reikalavimų nesilaikymą;

12.10. periodiškai inicijuoja EVIS administratoriaus, EVIS paslaugos teikėjo (-ų) administratoriaus (-ių) ir EVIS vidinių naudotojų mokymus elektroninės informacijos saugos klausimais, įvairiais būdais informuoja juos apie elektroninės informacijos saugos problemas (teminiai seminarai, atmintinės priimtiems naujiems darbuotojams ir pan.);

12.11. atlieka kitas EVIS tvarkytojo vadovo pavestas užduotis, saugos dokumentuose ir kituose saugos reikalavimus nustatančiuose teisės aktuose jam priskirtas funkcijas.

13. Saugos įgaliotinis negali atlikti EVIS administratoriaus funkcijų.

14. EVIS administratoriaus funkcijos ir atsakomybė:

14.1. atlieka EVIS vidiniams naudotojams priskirtų funkcijų ir suteiktų teisių atitikties vertinimą, administruoja šias teises;

14.2. rengia ir tikrina EVIS sudarančių komponentų sąranką, teikia saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę;

14.3. ne rečiau kaip kartą per metus ir (arba) atlikus EVIS pakeitimus tikrina (peržiūri) EVIS sąranką ir EVIS būsenos rodiklius;

14.4. pagal kompetenciją reaguoja į saugos incidentus, registruoja juos ir informuoja saugos įgaliotinį apie nustatytus saugos politikos pažeidimus, teikia pasiūlymus dėl minėtų incidentų šalinimo, taip pat informuoja saugos įgaliotinį apie nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones;

14.5. nustato EVIS pažeidžiamas vietas ir informuoja apie jas saugos įgaliotinį;

14.6. užtikrina, kad būtų laikomasi saugos dokumentų ir kitų teisės aktų reikalavimų;

14.7. vykdo saugos įgaliotinio nurodymus ir pavedimus, susijusius su EVIS duomenų saugos užtikrinimu;

14.8. įregistruoja ir išregistruoja EVIS vidinius naudotojus, atsako už prieigos prie EVIS teisių nustatymą;

14.9. kontroliuoja ir prižiūri programinės ir kompiuterinės įrangos diegimo procesus;

14.10. tikrina pranešimus apie serverių operacinių sistemų ir duomenų bazių valdymo sistemų klaidas ir imasi būtinų priemonių, kad būtų išvengta galimų gedimų;

14.11. užtikrina visų prisijungimo vardų, slaptažodžių apsaugą;

14.12. teikia Direkcijos vadovui ir saugos įgaliotiniui pasiūlymus dėl EVIS kūrimo, funkcionalumo užtikrinimo, priežiūros ir duomenų saugos klausimų;

14.13. dalyvauja atkuriant EVIS elektroninę informaciją iš elektroninės informacijos atsarginių kopijų;

14.14. kontroliuoja, kad EVIS elektroninės informacijos duomenų bazė būtų laiku sunaikinta.

14.15. tvarko EVIS eksploatacijos žurnalą;

14.16. atlieka kitas Direkcijos vadovo pavestas užduotis ir kitas Saugos nuostatuose ir kituose saugos dokumentuose administratoriui priskirtas funkcijas.

15. EVIS paslaugos teikėjo administratoriaus funkcijos ir atsakomybė:

15.1. vykdo EVIS paslaugos teikėjo darbuotojų, EVIS naudojančius sutartiniams įsipareigojimams vykdyti, EVIS atliekamų veiksmų kontrolę;

15.2. rengia ir tikrina EVIS sudarančių komponentų sąranką, teikia EVIS administratoriui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę;

15.3. prižiūri EVIS sudarančias dalis (kompiuterius, operacines sistemas, duomenų bazių valdymo sistemas, taikomųjų programų sistemas, ugniasienes, įsilaužimo aptikimo sistemas, duomenų perdavimo tinklus ir kt.), kontroliuoja EVIS ir ją sudarančių komponentų nepertraukiamą veikimą ir už tai atsako;

15.4. reaguoja į saugos incidentus, registruoja juos ir informuoja EVIS administratorių apie nustatytus saugos politikos pažeidimus, teikia pasiūlymus dėl minėtų incidentų šalinimo, taip pat informuoja EVIS administratorių apie nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones;

15.5. užtikrina, kad būtų laikomasi saugos dokumentų ir kitų teisės aktų reikalavimų;

15.6. įdiegia programinės įrangos atnaujinimus, nustato automatinio atnaujinimo procedūras;

15.7. kontroliuoja ir prižiūri programinės ir kompiuterinės įrangos diegimo procesus;

15.8. tikrina pranešimus apie serverių operacinių sistemų ir duomenų bazių valdymo sistemų klaidas ir imasi būtinų priemonių, kad būtų išvengta galimų gedimų;

15.9. užtikrina visų prisijungimo vardų, slaptažodžių apsaugą;

15.10. daro atsargines EVIS elektroninės informacijos kopijas;

15.11. atsako už EVIS elektroninės informacijos atsarginių kopijų darymą, tinkamumą ir saugojimą bei naikinimą;

15.12. atlieka kitas Direkcijos ir EVIS paslaugos teikėjo sutartyje numatytas funkcijas, Saugos nuostatuose ir kituose saugos dokumentuose EVIS paslaugos teikėjo administratoriui priskirtas funkcijas.

16. Teisės aktų, kuriais vadovaujamasi tvarkant EVIS elektroninę informaciją ir užtikrinant jų saugumą, sąrašas:

16.1. 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);

16.2. Valstybės informacinių išteklių valdymo įstatymas;

16.3. Kibernetinio saugumo įstatymas;

16.4. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas 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“;

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

16.6. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašas, patvirtintas 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“;

16.7. Lietuvos standartai LST ISO/IEC 27002 ir LST ISO/IEC 27001, Lietuvos ir tarptautiniai „Informacinės technologijos. Saugumo metodai“ grupės standartai, nustatantys saugų informacinės sistemos duomenų tvarkymą;

16.8. EVIS nuostatai;

16.9. Saugos nuostatai;

16.10. saugos politikos įgyvendinamieji dokumentai.

II SKYRIUS
EVIS ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

17. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Elektroninės informacijos klasifikavimo gairių aprašas), 10 punktu, EVIS tvarkoma informacija priskiriama mažiausios svarbos informacijos kategorijai.

18. Vadovaujantis Elektroninės informacijos klasifikavimo gairių aprašo 12.4 papunkčiu, EVIS pagal joje tvarkomos informacijos svarbą priskiriama ketvirtajai kategorijai (kurioje tvarkoma mažiausios svarbos informacija).

19. Saugos įgaliotinis, atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacinės technologijos. Saugumo metodai“ grupės standartus, kasmet organizuoja EVIS rizikos įvertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį rizikos įvertinimą. EVIS rizikos įvertinimas atliekamas pagal kokybinį rizikos vertinimo metodą. Kartu su pagrindiniu EVIS rizikos įvertinimu organizuojamas ir atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos EVIS kibernetiniam saugumui, vertinimas. EVIS tvarkytojo rašytiniu pavedimu EVIS rizikos įvertinimą gali atlikti pats saugos įgaliotinis.

20. EVIS rizikos įvertinimo rezultatai pateikiami rizikos įvertinimo ataskaitoje ir ji pateikiama EVIS tvarkytojo vadovui. Rizikos įvertinimo ataskaita rengiama įvertinant rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausi rizikos veiksniai yra šie:

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

20.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis EVIS elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

20.3. 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.

21. Rizikos įvertinimo metu atliekamos veiklos:

21.1. EVIS sudarančių informacinių išteklių inventorizacija;

21.2. įtakos EVIS veiklai vertinimas;

21.3. grėsmės ir pažeidimų analizė;

21.4. liekamosios rizikos vertinimas.

22. Atsižvelgdamas į rizikos įvertinimo ataskaitą, EVIS valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių ir kitų išteklių poreikis EVIS rizikos valdymo priemonėms įgyvendinti.

23. Pagrindiniai EVIS elektroninės informacijos saugos priemonių parinkimo principai yra šie:

23.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

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

23.3. esant galimybei, turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

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

25. Siekiant užtikrinti Saugos nuostatų ir saugos politikos įgyvendinamųjų dokumentų nuostatų įgyvendinimo kontrolę, ne rečiau kaip kartą per 2 metus organizuojamas informacinių technologijų saugos atitikties vertinimas, vadovaujantis Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta 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“.

26. Atliekant EVIS informacinių technologijų saugos atitikties vertinimą:

26.1. įvertinama esamos EVIS elektroninės informacijos saugos situacijos atitiktis EVIS saugos dokumentams ir kitiems elektroninės informacijos saugą reglamentuojantiems teisės aktams;

26.2. inventorizuojama EVIS techninė ir programinė įranga;

26.3. peržiūrima EVIS administratoriui, EVIS paslaugos teikėjo administratoriui, EVIS vidiniams naudotojams ir EVIS elektroninės paslaugos gavėjams (Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos nuostatų, patvirtintų Lietuvos Respublikos susisiekimo ministro 2020 m. rugpjūčio 19 d. įsakymu Nr. 3-461 „Dėl Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos nuostatų ir Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos duomenų saugos nuostatų patvirtinimo“, 8.6 papunktis) (toliau – EVIS išoriniai naudotojai) suteiktų teisių atitiktis jų atliekamoms funkcijoms;

26.4. duomenų saugos požiūriu patikrinama EVIS techninė ir programinė įranga: visos tarnybinės stotys ir ne mažiau kaip 10 proc. atsitiktinai parinktų EVIS vidinių naudotojų darbo vietų;

26.5. įvertinamas pasirengimas užtikrinti EVIS veiklos tęstinumą įvykus saugos incidentui.

27. Atlikus EVIS informacinių technologijų saugos atitikties vertinimą, parengiama informacinių technologijų saugos atitikties vertinimo ataskaita ir pateikiama Direkcijos vadovui, taip pat parengiamas pastebėtų trūkumų šalinimo planas. EVIS valdytojo vadovas patvirtina šį planą, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminus.

28. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas EVIS 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.

29. Prireikus saugos įgaliotinis gali organizuoti neeilinį EVIS informacinių technologijų saugos atitikties vertinimą.

30. Neeilinis EVIS informacinių technologijų saugos atitikties vertinimas atliekamas:

30.1. įvykus EVIS techninės ar programinės įrangos pokyčiams, kurie gali turėti įtakos EVIS veikimui;

30.2. paaiškėjus naujoms tendencijoms informacinių technologijų saugos srityje, dėl kurių kiltų grėsmė EVIS techninei, programinei įrangai ar EVIS tvarkomai elektroninei informacijai;

30.3. po saugos incidento, kurio metu buvo sutrikdyta EVIS veikla, sugadinta ar prarasta EVIS elektroninė informacija.

31. Pokyčiai, galintys daryti neigiamą įtaką elektroninės informacijos konfidencialumui, vientisumui ar prieinamumui, turi būti patikrinti bandomojoje aplinkoje, kurioje nėra konfidencialių ir asmens duomenų ir kuri atskirta nuo eksploatuojamos EVIS.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

32. Nustatomi šie EVIS naudojamos programinės įrangos reikalavimai:

32.1. EVIS naudojama programinė įranga turi atitikti programinės įrangos saugos gerąją praktiką, kuriant programinę įrangą taikomą saugos gerąją praktiką, programinės įrangos kūrimo struktūras, standartus.

32.2. Specifiniai saugos reikalavimai turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose.

32.3. Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos.

32.4. Programinės įrangos kūrimo, testavimo ir verifikacijos etapai turi vykti atsižvelgiant į pagrindinius saugos reikalavimus.

32.5. Prieš pradedant naudoti programinę įrangą, turi būti atliktas šios programinės įrangos pažeidžiamumo, pritaikomumo ir infrastruktūros atsparumo skverbimuisi įvertinimas. Programinė įranga negali būti patvirtinta, kol nėra pasiektas reikiamas saugumo lygis.

32.6. Turi būti atliekami periodiški infrastruktūros atsparumo skverbimuisi testavimai.

33. Metodai ir priemonės, kurie taikomi užtikrinant prieigą prie EVIS:

33.1. EVIS vidiniai naudotojai ir EVIS išoriniai naudotojai (toliau – EVIS naudotojai) privalo turėti galimybę naudotis tik tokiomis teisėmis ir tais duomenimis, kurie jiems numatyti nustačius prieigos prie EVIS teises, įgyvendinant principą „būtina žinoti“.

33.2. EVIS priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą EVIS administratoriaus ar EVIS paslaugos teikėjo administratoriaus klasifikatorių, kuriuo naudojantis nebūtų galima atlikti EVIS naudotojo funkcijų.

33.3. Kiekvienas EVIS naudotojas turi būti EVIS unikaliai identifikuojamas. EVIS vidinis naudotojas arba EVIS išorinis naudotojas, kuris yra susikūręs savo paskyrą EVIS, turi patvirtinti savo tapatybę slaptažodžiu, EVIS vidiniam naudotojui suteiktas pirminis slaptažodis turi būti pakeistas pirmo prisijungimo metu.

33.4. EVIS turi registruoti paskutinį EVIS elektroninės informacijos pakeitimą atlikusį EVIS naudotoją ir pakeitimo laiką.

33.5. Prieigą prie EVIS suteikia, apriboja ir panaikina pagal savo kompetenciją EVIS administratorius ar EVIS paslaugos teikėjo administratorius.

33.6. Teisė dirbti su konkrečia elektronine informacija suteikiama konkrečiam darbuotojui.

33.7. Patalpose, kuriose yra EVIS duomenų centras, turi būti įrengti ir prie pastato signalizacijos ir apsaugos tarnybų prijungti gaisro ir įsilaužimo jutikliai.

33.8. Duomenų centro patalpose turi būti įrengta stebėjimo sistema su įrašymo funkcija.

34. Programinės įrangos, skirtos EVIS ir kompiuterizuotoms darbo vietoms (toliau – KDV) apsaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos:

34.1. EVIS turi būti naudojama antivirusinė programinė įranga, skirta EVIS apsaugoti nuo kenksmingos programinės įrangos.

34.2. Antivirusinė programinė įranga turi būti atnaujinama automatiškai ne rečiau kaip kartą per parą.

34.3. EVIS vidinių naudotojų kompiuteriuose naudojama įranga, skirta KDV apsaugoti nuo kenksmingos programinės įrangos, turi apsaugoti ir elektroninio pašto programinę įrangą nuo nepageidaujamo pašto ar kenksmingų programų patekimo į KDV.

34.4. Atsiradus požymių, kad KDV yra kenksmingų programų, turi būti patikrinami visi KDV standieji diskai, naudojama programinė įranga, skirta EVIS ir KDV apsaugoti nuo kenksmingos programinės įrangos.

34.5. KDV esančios programinės įrangos, skirtos EVIS ir KDV apsaugoti nuo kenksmingos programinės įrangos, nustatymai turi būti parinkti pagal rekomenduojamus tokios programinės įrangos gamintojų reikalavimus arba pagal vidinio kompiuterių tinklo administratoriaus rekomendacijas.

34.6. Programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

34.7. Apsaugos sistema privalo automatiškai informuoti EVIS paslaugos teikėjo administratorių apie KDV ir tarnybines stotis, kuriose apsaugos sistema netinkamai funkcionuoja, yra išjungta arba neatsinaujino per 24 valandas.

34.8. EVIS operacinės sistemos ir naudojami programinės įrangos gamintojų rekomenduojami atnaujinimai turi būti įdiegiami operatyviai – ne vėliau kaip per 5 darbo dienas nuo programinės įrangos paketo išleidimo.

34.9. EVIS turi būti naudojama tik licencijuota programinė įranga.

35. Programinės įrangos, įdiegtos KDV ir tarnybinėse stotyse, naudojimo nuostatos:

35.1. EVIS naudojama tik legali programinė įranga.

35.2. Draudžiama diegti ir naudoti bet kokią programinę įrangą, keisti sistemos, kompiuterio ar programinės įrangos sistemų nustatymus. Programinę įrangą, reikalingą EVIS vidinio naudotojo funkcijoms atlikti, KDV diegia, atnaujina, kontroliuoja ir prižiūri EVIS paslaugos teikėjo administratorius. Kiti asmenys (paslaugų teikėjų specialistai) gali diegti programinę įrangą tik EVIS paslaugos teikėjo administratoriaus prižiūrimi.

35.3. Diegti ir naudoti programinę įrangą, nesusijusią su EVIS valdytojo ar EVIS tvarkytojų veikla ar EVIS vidinio naudotojo atliekamomis funkcijomis (žaidimų, bylų siuntimo, internetinių pokalbių programas ir kt.), draudžiama.

35.4. Programinė įranga yra nuolat atnaujinama laikantis gamintojo reikalavimų.

35.5. EVIS tarnybinėse stotyse negali būti įdiegta programinė įranga, kuri nesusijusi su EVIS veikla.

36. Leistinos kompiuterių (ypač nešiojamųjų) naudojimo ribos ir metodai, kuriais užtikrinamas saugus EVIS duomenų teikimas ir (ar) gavimas:

36.1. EVIS išoriniai naudotojai naudojasi prieiga prie EVIS per išorinį portalą. EVIS išoriniams naudotojams prisijungimo laikas nėra ribojamas.

36.2. Prie EVIS prisijungiama nuotoliniu būdu naudojant interneto naršyklę (*https* protokolą).

36.3. EVIS vidiniam naudotojui teisė dirbti su konkrečia elektronine informacija turi būti ribojama ar sustabdoma, kai EVIS vidinis naudotojas atostogauja, vykdomas EVIS vidinio naudotojo veiklos tyrimas ir pan. Pasibaigus tarnybos (darbo) santykiams, EVIS vidinio naudotojo teisė naudotis EVIS turi būti panaikinta.

36.4. Baigus darbą, turi būti imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo EVIS, įjungiama ekrano užsklanda su slaptažodžiu, dokumentai padedami į pašaliniams asmenims neprieinamą vietą.

36.5. EVIS vidiniam naudotojui 15 min. neatliekant jokių veiksmų, EVIS turi užsirakinti, kad toliau naudotis EVIS būtų galima tik pakartojus tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus.

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

37.1. Techninis nuotolinio prisijungimo sprendimas turi užtikrinti ne žemesnį nei vidiniam prisijungimui naudojamą saugumo lygį, t. y. turi būti naudojamos Saugos nuostatuose minimos priemonės ir duomenų šifravimas naudojantis virtualiu privačiu tinklu (angl. *virtual private network* – VPN).

37.2. EVIS vidiniams naudotojams, kuriems atliekant tiesiogines pareigas būtina prisijungti iš nutolusios darbo vietos, gali būti suteikiama nuotolinio prisijungimo prie EVIS galimybė.

37.3. Kompiuterinis tinklas, prie kurio prijungtos EVIS tarnybinės stotys ir EVIS vidinių naudotojų kompiuteriai, nuo viešojo interneto turi būti atskirtas ugniasienėmis ir įsilaužimų aptikimo ir prevencijos įranga, už kurios administravimą ir priežiūrą atsakingas EVIS paslaugos teikėjo administratorius.

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

37.5. Naudojamos turinio filtravimo sistemos.

38. Kompiuterių (įskaitant nešiojamuosius) naudojimo reikalavimai:

38.1. Stacionarieji ir nešiojamieji EVIS vidinių naudotojų kompiuteriai turi būti naudojami tik su tiesioginių pareigų atlikimu susijusiai veiklai. Iš kompiuterių, kurie perduodami remontui ar techninei priežiūrai, turi būti pašalinta visa riboto naudojimo EVIS elektroninė informacija.

38.2. Visiems EVIS vidinių naudotojų kompiuteriams turi būti naudojamos papildomos saugos priemonės, kuriomis patvirtinama kompiuterio naudotojo tapatybė.

38.3. EVIS vidiniai naudotojai, darbo funkcijoms atlikti naudojantys nešiojamuosius kompiuterius, išnešdami juos iš EVIS tvarkytojų patalpų, norėdami EVIS duomenis perduoti kompiuterių tinklais ne savo darbo vietoje, turi naudoti duomenų šifravimą, papildomą naudotojo tapatybės patvirtinimą, rakinimo įrenginį. Nešiojamojo kompiuterio pagrindinė įvesties ir išvesties sistema (BIOS) turi būti apsaugota slaptažodžiu ir nurodytas kietasis diskas kaip pirminis paleidimo įrenginys. Iš išorės prie EVIS duomenų bazės prisijungimas ribojamas. Nešiojamuosiuose kompiuteriuose ar išorinėse kompiuterinėse laikmenose esantys duomenys turi būti šifruojami. EVIS vidiniai naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo.

39. Užtikrinant saugų elektroninės informacijos teikimą kitoms valstybės institucijoms ir (ar) gavimą iš jų, naudojamas šifruotas VPN arba Saugus valstybinis duomenų perdavimo tinklas (toliau – SVDPT). Elektronine informacija keičiamasi per saugųjį HTTP (angl. *Hypertext Transfer Protocol Secure*) duomenų perdavimo protokolą (HTTPS) žiniatinklio paslaugų metodu (XML formatu) arba duomenų bazių užklausomis. Duomenys teikiami ir (ar) gaunami automatizuotomis priemonėmis tik pagal duomenų teikimo sutartyje nustatytas specifikacijas, duomenų perdavimo sąlygas ir tvarką.

40. Metodai, kuriais gali būti užtikrinamas saugus EVIS elektroninės informacijos teikimas ir (ar) gavimas:

40.1. EVIS elektroninė informacija perduodama automatiniu būdu (naudojant TCP/IP protokolą) realiuoju laiku arba asinchroniniu režimu pagal EVIS duomenų teikimo ir gavimo sutartis, kuriose nustatytos perduodamų duomenų specifikacijos, perdavimo sąlygos ir tvarka.

40.2. Už EVIS elektroninės informacijos teikimo ir gavimo sutartyse nurodomų saugos reikalavimų nustatymą, suformulavimą ir įgyvendinimo organizavimą atsakingas saugos įgaliotinis.

40.3. EVIS elektroninei informacijai perduoti naudojamas SVDPT arba kitas šifruotas perdavimo kanalas, užtikrinantis saugų elektroninės informacijos perdavimą.

41. Pagrindiniai atsarginių EVIS elektroninės informacijos kopijų darymo ir atkūrimo reikalavimai:

41.1. EVIS atsarginės kopijos turi būti daromos automatiškai kartą per parą.

41.2. Privalo būti visos saugomos elektroninės informacijos rezervinio kopijavimo funkcija.

41.3. EVIS administratorius privalo turėti galimybę inicijuoti elektroninės informacijos atkūrimo iš rezervinės kopijos procedūrą pasirinktinai iš turimų rezervinių kopijų sąrašo. Atkūrus elektroninę informaciją privalo būti užtikrintas ir išlaikytas elektroninės informacijos vientisumas ir integralumas.

41.4. EVIS elektroninė informacija EVIS naudotojams turi būti prieinama ne mažiau kaip 99,30 proc. laiko per mėnesį.

41.5. Jeigu neveikia EVIS ar jos dalis ir dėl to nutrūksta transporto priemonių eilių elektroninis reguliavimas, ne vėliau kaip per 2 valandas turi būti atkurtas EVIS funkcionalumas. Poste priešais pasienio kontrolės punktą sutartinius įsipareigojimus vykdantiems EVIS paslaugos teikėjo darbuotojams turi būti sudaryta galimybė nuolat gauti duomenis apie registruotas transporto priemones iš atsarginio informacijos šaltinio, kuriame reguliariai išsaugomi duomenys apie registruotas transporto priemones. Vadovaudamiesi šiais duomenimis, EVIS paslaugos teikėjo darbuotojai leis įvažiuoti transporto priemonėms į pasienio kontrolės punktą, kol bus atkurtas EVIS funkcionalumas.

41.6. Elektroninė informacija atsarginėse kopijose turi būti šifruota (šifravimo raktai turi būti saugomi atskirai nuo atsarginių kopijų).

41.7. EVIS elektroninės informacijos atsarginės kopijos yra daromos ir saugomos taip, kad jos nebūtų prieinamos tretiesiems asmenims, kurie neturi teisės su jomis dirbti.

41.8. EVIS atsarginės elektroninės informacijos kopijos turi būti laikomos atskiroje (nuo pagrindinių duomenų) patalpoje ir saugomos užrakintoje nedegioje spintoje. Už atsarginių kopijų darymą ir atkūrimą atsakingas EVIS paslaugos teikėjo administratorius.

41.9. Atkūrimo iš atsarginių kopijų funkcija privalo būti išbandoma ne rečiau kaip kartą per metus. Testavimo eiga ir rezultatai įforminami kopijų darymo žurnale. Duomenų atkūrimo bandymą organizuoja saugos įgaliotinis.

42. Nustatomi duomenų naikinimo ir šalinimo reikalavimai:

42.1. Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinta visa joje esanti elektroninė informacija, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Jeigu to padaryti neįmanoma (pvz., DVD laikmenos), duomenų laikmenos turi būti fiziškai sunaikinamos be galimybės atkurti duomenis.

42.2. Prieš šalinant laikmenas, turi būti atlikti visų šalinamų laikmenų daugybiniai programinės įrangos perrašymai.

42.3. Jeigu saugiems duomenų naikinimo ir šalinimo duomenų laikmenose darbams atlikti yra pasitelkiamos trečiosios šalies paslaugos, turi būti sudaryta atitinkama paslaugų sutartis.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

43. Saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus ir metodus, rizikų valdymą, kiekvienais metais tobulinti kvalifikaciją elektroninės informacijos saugos srityje ir savo darbe vadovautis Reglamentu (ES) 2016/679, saugos dokumentais, Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu 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“, Informacinių technologijų saugos atitikties vertinimo metodika ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais elektroninės informacijos saugą, kibernetinį saugumą, taip pat būti susipažinęs su esminiais EVIS elektroninės informacijos saugos reikalavimais. Saugos įgaliotinis privalo sugebėti prižiūrėti, kaip įgyvendinama saugos politika.

44. Saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą galiojančią 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 nuobaudos paskyrimo praėję mažiau kaip vieni metai.

45. EVIS administratorius ar EVIS paslaugos teikėjo administratorius privalo išmanyti darbą su kompiuterių tinklais ir mokėti užtikrinti jų saugumą, būti susipažinęs su duomenų bazių

administravimo ir priežiūros pagrindais, gebėti užtikrinti techninės ir programinės įrangos nepertraukiamą funkcionavimą bei saugą, stebėti techninės ir programinės įrangos veikimą, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, sutrikimų bei saugos incidentų diagnostiką ir šalinimą.

46. Visi EVIS vidiniai naudotojai privalo turėti darbo kompiuteriu įgūdžių.

47. EVIS vidiniai naudotojai privalo rūpintis tvarkomų duomenų saugumu. EVIS vidiniai naudotojai turi būti susipažinę su Reglamentu (ES)2016/679, Saugos nuostatais ir saugos politiką reglamentuojančiais teisės aktais. Tvarkyti EVIS elektroninę informaciją gali tik EVIS vidiniai naudotojai, pasirašę pasižadėjimą saugoti asmens duomenų paslaptį. Ši pareiga galioja ir pasitraukus iš valstybės tarnybos, perėjus dirbti į kitas pareigas arba pasibaigus darbo, sutartiniams ar kitiems santykiams.

48. EVIS vidiniai naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias EVIS saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti EVIS administratoriui, o jo nesant – saugos įgaliotiniui. Jeigu saugos įgaliotinis nebuvo informuotas apie šiame punkte nurodytus pažeidimus, EVIS administratorius informuoja saugos įgaliotinį apie šiuos pažeidimus.

49. EVIS vidinių naudotojų mokymai organizuojami taip, kaip numatyta Saugos nuostatų 12.10 papunktyje, ne rečiau kaip kartą per metus.

V SKYRIUS
EVIS VIDINIŲ NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

50. Direkcijos vadovas užtikrina, kad EVIS vidiniai naudotojai būtų supažindinti su saugos dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą ir atsakomybę už šių teisės aktų nuostatų pažeidimus.

51. Už EVIS vidinių naudotojų, EVIS administratoriaus ir EVIS paslaugos teikėjo (-ų) administratoriaus (-ių) supažindinimą su saugos dokumentais ir atsakomybe, kylančia dėl jų pažeidimo, atsakingas saugos įgaliotinis.

52. EVIS administratorių ir EVIS paslaugos teikėjo (-ų) administratorių (-ius) su saugos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodymą, supažindina saugos įgaliotinis per 10 darbo dienų nuo EVIS administratoriaus ar EVIS paslaugos teikėjo administratoriaus (-ių) paskyrimo.

53. EVIS vidinius naudotojus su saugos dokumentais ir teisės aktais, reglamentuojančiais EVIS elektroninės informacijos saugą, saugos įgaliotinis pasirašytinai supažindina prieš sukurdamas EVIS vidinio naudotojo prisijungimo duomenis.

54. Pakartotinai su saugos dokumentais ir teisės aktais, reglamentuojančiais EVIS elektroninės informacijos saugą, saugos įgaliotinis pasirašytinai supažindina EVIS vidinius naudotojus ir EVIS administratorių ar EVIS paslaugos teikėjo (-ų) administratorių (-ius) kitą darbo dieną po saugos dokumentų ir teisės aktų, reglamentuojančių EVIS elektroninės informacijos saugą, priėmimo (išdėstymo nauja redakcija), pakeitimo ar pripažinimo netekusiais galios.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

55. Saugos įgaliotinis organizuoja saugos dokumentų persvarstymą ne rečiau kaip kartą per metus. Saugos dokumentai turi būti persvarstomi atlikus rizikos analizę ar informacinių technologijų saugos atitikties vertinimą, pasikeitus saugos politiką reglamentuojantiems teisės aktams, įvykus esminiams organizaciniams, technologiniams ar kitiems EVIS pokyčiams, po įvykusio kibernetinio incidento.

56. Saugos įgaliotinis, EVIS administratorius, EVIS paslaugos teikėjo (-ų) administratorius (-iai), EVIS vidiniai naudotojai ir kiti subjektai, kuriems taikomi Saugos nuostatų reikalavimai, pažeidę saugos dokumentų ir kitų teisės aktų, reglamentuojančių saugų elektroninės informacijos tvarkymą, reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2021 m. birželio 29 d. raštu Nr. (4.1E) 6K-518

Pakeitimai:

1.
Lietuvos Respublikos susisiekimo ministerija, Įsakymas
Nr. 3-361, 2021-07-21, paskelbta TAR 2021-07-21, i. k. 2021-16185
Dėl Lietuvos Respublikos susisiekimo ministro 2020 m. rugpjūčio 19 d. įsakymo Nr. 3-461 „Dėl Pasienio kontrolės punktų informacinės sistemos modernizavimo, Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos nuostatų ir Transporto priemonių, laukiančių kirsti Lietuvos Respublikos valstybės sieną, eilių valdymo informacinės sistemos saugos nuostatų patvirtinimo“ pakeitimo