PATVIRTINTA
Lietuvos Respublikos
vidaus reikalų ministro
2008 m. vasario 8 d. įsakymu Nr. 1V-57

LIETUVOS RESPUBLIKOS KELIŲ TRANSPORTO PRIEMONIŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos kelių transporto priemonių registro duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Lietuvos Respublikos kelių transporto priemonių registro (toliau – KTPR) saugos politiką.

2. Saugos nuostatuose vartojamos sąvokos:

KTPR naudotojas – KTPR tvarkymo įstaigos ir KTPR duomenų gavėjo valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, kuris teisės aktų nustatyta tvarka turi teisę naudotis šio registro ištekliais numatytoms funkcijoms atlikti.

Kitos Saugos nuostatuose vartojamos sąvokos atitinka Bendruosiuose elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuose, patvirtintuose Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891) (toliau – Saugos reikalavimai), Lietuvos Respublikos kelių transporto priemonių registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2005 m. lapkričio 28 d. nutarimu Nr. 1286 (Žin., 2005, Nr. 141-5080), Saugos dokumentų turinio gairėse, patvirtintose Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070), ir kituose teisės aktuose vartojamas sąvokas.

3. KTPR duomenų saugos tikslas – užtikrinti KTPR duomenų konfidencialumą, prieinamumą ir vientisumą.

4. KTPR duomenų saugos užtikrinimo prioritetinės kryptys:

4.1. KTPR duomenų tvarkymui naudojamos techninės ir programinės įrangos kontrolė;

4.2. KTPR duomenų tvarkymo kontrolė;

4.3. naudojimosi KTPR duomenimis kontrolė.

5. KTPR duomenų saugai užtikrinti kompleksiškai naudojamos administracinės, techninės ir programinės priemonės.

6. KTPR vadovaujančioji tvarkymo įstaiga – Lietuvos Respublikos vidaus reikalų ministerija atlieka šias funkcijas, susijusias su KTPR duomenų sauga:

6.1. priima sprendimą dėl KTPR informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

6.2. atlieka kitas Saugos nuostatų, Saugos reikalavimų, KTPR nuostatų ir kitų teisės aktų nustatytas funkcijas.

7. KTPR tvarkymo įstaiga yra VĮ „Regitra“, kuri atlieka Saugos nuostatų, Saugos reikalavimų, KTPR nuostatų ir kitų teisės aktų nustatytas funkcijas, susijusias su KTPR duomenų sauga.

8. Saugos įgaliotinis atlieka šias funkcijas, susijusias su KTPR duomenų sauga:

8.1.teikia KTPR vadovaujančiajai tvarkymo įstaigai pasiūlymus dėl KTPR duomenų saugai užtikrinti reikalingų techninių ir programinių priemonių įsigijimo, įdiegimo ir modernizavimo;

8.2. atlieka kitas Saugos nuostatų, Saugos reikalavimų ir kitų teisės aktų nustatytas funkcijas.

9. KTPR administratoriai atlieka KTPR priežiūros funkcijas, teikia siūlymus saugos įgaliotiniui dėl KTPR saugos priemonių ir atlieka kitas Saugos reikalavimų ir kitų teisės aktų nustatytas funkcijas.

10. Teisės aktai, kuriais vadovaujantis tvarkomi KTPR duomenys ir užtikrinama jų sauga:

10.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (Žin., 1996, Nr. 63-1479; 2003, Nr. 15-597);

10.2. Lietuvos Respublikos valstybės registrų įstatymas (Žin., 1996, Nr. 86-2043; 2004, Nr. 124-4488);

10.3. Saugos reikalavimai;

10.4. KTPR nuostatai;

10.5. KTPR duomenų saugaus tvarkymo taisyklės;

10.6. KTPR naudotojų administravimo taisyklės;

10.7. Lietuvos standartai LST ISO/IEC 17799:2006 ir LST ISO/IEC 27001:2006 bei Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, reglamentuojantys saugų duomenų tvarkymą;

10.8. kiti teisės aktai, reglamentuojantys KTPR duomenų tvarkymo teisėtumą, KTPR naudotojų veiklą ir KTPR duomenų saugos valdymą.

II. KTPR DUOMENŲ SAUGOS VALDYMAS

11. Atsižvelgiant į galimas KTPR duomenų savybių (vientisumo, konfidencialumo ir prieinamumo) praradimo pasekmes ir tai, kad KTPR yra valstybės registras, KTPR priskiriamas antrai informacinių sistemų kategorijai pagal Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairių, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymu Nr. 1V-247 (Žin., 2007, Nr. 78-3160), 3.2.1 ir 3.2.6 p.

12. KTPR saugos priemonės parenkamos įvertinus galimus rizikos veiksnius, susijusius su KTPR duomenų vientisumu, konfidencialumu ir prieinamumu.

13. Pagrindinės KTPR rizikos mažinimo priemonės išdėstomos rizikos įvertinimo ataskaitoje. KTPR rizikos vertinime dalyvauja VĮ „Regitra“ centrinio registratoriaus ir teritorinių registratorių vadovai ar jų įgalioti asmenys. Saugos įgaliotinis rengia registro rizikos įvertinimo ataskaitą kasmet iki liepos 1 dienos, o prireikus ir neeilinio vertinimo ataskaitą iki KTPR vadovaujančios tvarkymo įstaigos nurodytos datos. Įvertinami galintys turėti įtakos KTPR duomenų saugai rizikos veiksniai, iš kurių svarbiausi išvardyti Saugos reikalavimų 31 punkte.

14. KTPR vadovaujančioji tvarkymo įstaiga, atsižvelgdama į saugos įgaliotinio parengtą KTPR rizikos įvertinimo ataskaitą, prireikus tvirtina VĮ „Regitra“ parengtą KTPR rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

15. KTPR rizikos veiksnių vertinimui taikoma kokybinė rizikos vertinimo metodika. Pagrindiniai rizikos vertinimo kriterijai pasirenkami atliekant KTPR rizikos vertinimą pagal KTPR rizikos vertinimo strategiją.

16. Siekiant užtikrinti Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose išdėstytų nuostatų įgyvendinimo kontrolę, vidaus reikalų ministro patvirtintos informacinių technologijų saugos atitikties vertinimo metodikos nustatyta tvarka kasmet organizuojamas KTPR informacinių technologijų saugos reikalavimų atitikties vertinimas, kurio metu:

16.1. įvertinama realios KTPR duomenų saugos situacijos ir Saugos nuostatų bei kitų saugos politiką įgyvendinančių teisės aktų reikalavimų atitiktis;

16.2. inventorizuojama KTPR techninė ir programinė įranga;

16.3. tikrinama ne mažiau kaip 10 procentų KTPR naudotojų kompiuterinių darbo vietų ir KTPR tarnybinėse stotyse įdiegtos programos bei jų sąranka (konfigūracija);

16.4. patikrinama KTPR naudotojams suteiktų teisių tvarkyti KTPR ir atliekamų funkcijų atitiktis, prireikus KTPR naudotojų teisės praplečiamos arba apribojamos;

16.5. įvertinamas pasirengimas užtikrinti KTPR veiklos tęstinumą įvykus KTPR duomenų saugos incidentui.

17. Atlikus KTPR informacinių technologijų saugos reikalavimų atitikties vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato KTPR vadovaujančioji tvarkymo įstaiga.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

18. KTPR darbui turi būti naudojama tik legali programinė įranga.

19. KTPR tarnybinėse stotyse turi veikti tik licencijuota programinė įranga, kuri būtina KTPR veikimo ir administravimo bei tarnybinės stoties veiksmingumo užtikrinimui.

20. Darbo stotyse, kurios naudojamos KTPR duomenims tvarkyti, privalo veikti programinė įranga, skirta kovai su kenksminga programine įranga, atnaujinama automatiniu būdu ne rečiau kaip kas tris dienas.

21. KTPR programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims.

22. KTPR naudojamas VĮ „Regitra“ telekomunikacinis tinklas, turi būti atskirtas nuo kitų tinklų tinklo užkarda. Už šio telekomunikacinio tinklo administravimą ir priežiūrą atsako VĮ „Regitra“. Prieiga prie KTPR turi būti kontroliuojama naudojant VĮ „Regitra“ telekomunikacinio tinklo filtravimo įrangą. Už filtravimo techninės ir programinės įrangos priežiūrą bei kenkėjišką veiklą ribojančios techninės ir programinės įrangos atnaujinimą atsakingi įgalioti KTPR administratoriai. Išimtinais atvejais (jei būtina KTPR veiklai užtikrinti) galimas KTPR administratorių prisijungimas prie KTPR nuotoliniu būdu, naudojant virtualų privatų tinklą.

23. Tiesioginė prieiga prie KTPR duomenų suteikiama įgyvendinus KTPR naudotojų identifikavimo priemones. Tiesioginė prieiga prie KTPR turi būti užtikrinama automatiniu būdu visą parą, darbo ir poilsio dienomis.

24. Perduodant KTPR duomenis automatiniu būdu prijungties režimu (angl. *on-line*) arba asinchroniniu režimu pagal KTPR duomenų teikimo sutartis, kuriose nustatytos perduodamų duomenų specifikacija, kopijų skaičius, kitos duomenų perdavimo sąlygos ir tvarka, naudojamas TCP/IP protokolas.

25. KTPR duomenys, perduodami ne per VĮ „Regitra“ telekomunikacinį tinklą, turi būti šifruojami; šį duomenų šifravimą privalo užtikrinti VĮ „Regitra“.

26. KTPR naudotojų nešiojamuosiuose kompiuteriuose, kurie skirti tarnybinėms funkcijoms vykdyti – KTPR duomenų perdavimui kompiuterių tinklais ne savo darbo vietoje, turi būti naudojamas kompiuterio įjungimo slaptažodis, papildomas KTPR naudotojo tapatybės patvirtinimas ir KTPR duomenų šifravimas.

27. Bendri KTPR duomenų kopijų darymo ir atkūrimo reikalavimai:

27.1. KTPR duomenų kopijos turi būti daromos automatiškai kiekvieną dieną;

27.2. kartą per savaitę yra daroma visų KTPR duomenų kopija;

27.3. duomenų atkūrimo iš atsarginių kopijų testavimas turi būti atliekamas ne rečiau kaip kartą per šešis mėnesius;

27.4. turi būti tikrinamas KTPR duomenų kopijų išsamumas ir vientisumas;

27.5. KTPR duomenų kopijų kūrimą, sunaikinimą, atkūrimą ir saugojimą atlieka KTPR administratorius, turintis tam suteiktus įgaliojimus.

IV. REIKALAVIMAI PERSONALUI IR SUPAŽINDINIMO SU SAUGOS REIKALAVIMAIS TVARKA

28. Saugos įgaliotinis privalo gerai žinoti elektroninės informacijos saugos principus, saugos užtikrinimo metodus bei išmanyti Lietuvos Respublikos ir Europos Sąjungos teisės aktus, susijusius su duomenų saugos politika.

29. KTPR administratoriai privalo išmanyti pagrindinius elektroninės informacijos saugos principus, darbą su duomenų perdavimo tinklais, užtikrinti jų saugą, taip pat išmanyti duomenų bazių administravimo ir priežiūros pagrindus.

30. KTPR naudotojai turi turėti atitinkamą kvalifikaciją (informacinių technologijų vartotojų kvalifikacijos kursai, pradinis saugaus darbo su duomenimis mokymas, Europos kompiuterio vartotojo pažymėjimas ar pan.) ir patirties (darbo su atitinkamomis operacinėmis sistemomis, taikomosiomis programomis ir pan.).

31. KTPR naudotojai turi būti pasirašytinai susipažinę su Saugos nuostatais ir kitais saugos politiką įgyvendinančiais teisės aktais.

32. KTPR naudotojų supažindinimą su Saugos nuostatais ir kitais KTPR saugos politiką įgyvendinančiais teisės aktais ir atsakomybe už šių reikalavimų nesilaikymą organizuoja saugos įgaliotinis. Saugos įgaliotinis raštu informuoja KTPR naudotojus apie Saugos nuostatų pakeitimus ar kitų KTPR saugos politiką įgyvendinančių teisės aktų pripažinimą netekusiais galios, keitimą ar priėmimą.

33. KTPR naudotojams turi būti nuolat rengiami duomenų saugos mokymai, įvairiais būdais primenama apie saugos problematiką (pvz., priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės ir pan.).

V. BAIGIAMOSIOS NUOSTATOS

34. KTPR saugos įgaliotinis, KTPR administratoriai, KTPR naudotojai, pažeidę Saugos nuostatų ar kitų KTPR saugos politiką įgyvendinančių teisės aktų reikalavimus, atsako įstatymų nustatyta tvarka.

_____