**VALSTYBINĖS DUOMENŲ APSAUGOS INSPEKCIJOS DIREKTORIUS**

# ĮSAKYMAS DĖL VALSTYBINĖS DUOMENŲ APSAUGOS INSPEKCIJOS DIREKTORIAUS 2008 M. LAPKRIČIO 12 D. ĮSAKYMO NR. 1T-12(1.12) „DĖL BENDRŲJŲ REIKALAVIMŲ ORGANIZACINĖMS IR TECHNINĖMS DUOMENŲ SAUGUMO PRIEMONĖMS PATVIRTINIMO“ PAKEITIMO

2014 m. gruodžio 18 d. Nr. 1T-74(1.12.E)
Vilnius

Įgyvendindamas Lietuvos Respublikos valstybės kontrolės 2013 m. gruodžio 11 d. valstybinio audito ataskaitos Nr. VA-P-90-3-21 „Automatiniu būdu tvarkomų asmens duomenų apsauga“ 2 priede Valstybinei duomenų apsaugos inspekcijai pateiktų rekomendacijų 2.1 punktą:

1. P a k e i č i u Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymą Nr. 1T-12(1.12) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms patvirtinimo“:

1.1. išdėstau antraštę taip:

„DĖL BENDRŲJŲ REIKALAVIMŲ ORGANIZACINĖMS IR TECHNINĖMS ASMENS DUOMENŲ SAUGUMO PRIEMONĖMS PATVIRTINIMO“;

1.2. išdėstau 1 punktą taip:

„1. T v i r t i n u Bendruosius reikalavimus organizacinėms ir techninėms asmens duomenų saugumo priemonėms (pridedama).“;

1.3. išdėstau nurodytuoju įsakymu patvirtintus Bendruosius reikalavimus organizacinėms ir techninėms asmens duomenų saugumo priemonėms nauja redakcija (pridedama).

2. N u s t a t a u, kad šis įsakymas įsigalioja 2015 m. gegužės 1 d.

Direktorius Algirdas Kunčinas

PATVIRTINTA
Valstybinės duomenų apsaugos inspekcijos
direktoriaus 2008 m. lapkričio 12 d.
įsakymu Nr. 1T-71(1.12)
(Valstybinės duomenų apsaugos inspekcijos
direktoriaus 2014 m. gruodžio 18 d.
įsakymo Nr. 1T-74(1.12.E) redakcija)

# BENDRIEJI REIKALAVIMAI ORGANIZACINĖMS IR TECHNINĖMS ASMENS DUOMENŲ SAUGUMO PRIEMONĖMS

## I. BENDROSIOS NUOSTATOS

1. Bendrieji reikalavimai organizacinėms ir techninėms asmens duomenų saugumo priemonėms (toliau – Bendrieji reikalavimai) nustato bendruosius reikalavimus organizacinėms ir techninėms asmens duomenų saugumo priemonėms, kurias privalo įgyvendinti duomenų valdytojas ir duomenų tvarkytojas, siekdami apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo.

2. Bendrieji reikalavimai parengti vadovaujantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 30 straipsniu.

3. Duomenų valdytojai ir duomenų tvarkytojai, parinkdami organizacines ir technines asmens duomenų saugumo priemones, turi vadovautis šiais Bendraisiais reikalavimais.

4. Organizacinės ir techninės asmens duomenų saugumo priemonės turi užtikrinti tokį saugumo lygį, kuris atitiktų saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką.

5. Duomenų valdytojas ir duomenų tvarkytojas privalo užtikrinti, kad organizacinės ir techninės asmens duomenų saugumo priemonės būtų įgyvendintos, periodiškai peržiūrimos ir, esant reikalui, atnaujinamos.

6. Bendruosiuose reikalavimuose vartojamos sąvokos suprantamos taip, kaip jos yra apibrėžtos Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme ir kituose teisės aktuose.

7. Valstybės institucijos, valstybės įstaigos, valstybės įmonės, viešosios įstaigos, steigiančios, kuriančios ir (arba) tvarkančios valstybės registrus (kadastrus) (toliau – valstybės registras), žinybinius registrus, valstybės informacines sistemas ir kitas informacines sistemas (toliau – informacinė sistema), finansuojamas iš Lietuvos Respublikos valstybės biudžeto, Valstybinio socialinio draudimo fondo biudžeto, Privalomojo sveikatos draudimo fondo biudžeto ir kitų valstybės pinigų fondų ir Lietuvos Respublikos viešojo administravimo įstatymo nustatyta tvarka įgaliotoms atlikti viešąjį administravimą, valstybės ir savivaldybių įmonės, savivaldybių įstaigos ir viešosios įstaigos, kuriančios kitas informacinių technologijų priemones, kuriomis apdorojama informacija, valdoma valstybės ir savivaldybių įmonių, savivaldybių įstaigų ir viešųjų įstaigų, atliekančių teisės aktų joms nustatytas funkcijas, jeigu išlaidos, patirtos kuriant tokias informacinių technologijų priemones, finansuojamos iš Lietuvos Respublikos valstybės biudžeto, Valstybinio socialinio draudimo fondo biudžeto, Privalomojo sveikatos draudimo fondo biudžeto ar kitų valstybės pinigų fondų arba apdorojant informaciją informacinių technologijų priemonėmis per valstybės informacinių sistemų ar registrų sąveiką reikia gauti duomenis iš valstybės informacinių sistemų ir (arba) registrų (toliau – institucijos), kurios privalo vadovautis 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, atsižvelgiant į automatiniu būdu tvarkomų asmens duomenų saugumo lygį, turi įgyvendinti Bendrųjų reikalavimų 14.4–14.6, 15.1, 15.3 papunkčiuose nurodytas organizacines ir

technines asmens duomenų saugumo priemones, taip pat rekomenduojama įgyvendinti ir Bendrųjų reikalavimų 16.3–16.4 papunkčiuose nurodytas organizacines ir technines asmens duomenų saugumo priemones.

## II. ASMENS DUOMENŲ TVARKYMAS AUTOMATINIU BŪDU

8. Organizacinės ir techninės asmens duomenų saugumo priemonės turi būti išdėstytos rašytinės (popierinės ar elektroninės) formos dokumente (duomenų valdytojo patvirtintose asmens duomenų tvarkymo taisyklėse, duomenų valdytojo ir duomenų tvarkytojo sudarytoje sutartyje ir pan.), kuriame nurodoma:

8.1. duomenų valdytojas ir jo atliekamos funkcijos tvarkant asmens duomenis, turimos teisės ir pareigos;

8.2. duomenų tvarkytojas (-ai) (jei toks (tokie) yra) ir jo (jų) atliekamos funkcijos tvarkant asmens duomenis, turimos teisės ir pareigos;

8.3. teisės aktai ir standartai (jeigu jais vadovaujamasi), kuriais vadovaujamasi tvarkant asmens duomenis;

8.4. apibrėžtas (-i) ir teisėtas (-i) asmens duomenų tvarkymo tikslas (-ai);

8.5. baigtinis tvarkomų asmens duomenų sąrašas kiekvienu asmens duomenų tvarkymo tikslu;

8.6. automatiniu būdu tvarkomų asmens duomenų saugumo lygis (-iai);

8.7. konkretūs veiksmai ir (ar) procedūros, kurie leis įgyvendinti asmens duomenų tvarkymo reikalavimus (nurodyta, kaip, kokiais atvejais atliekamas asmens duomenų tikslinimas, taisymas, kada jie yra atnaujinami, kaip tvarkomi pasikeitę asmens duomenys ir pan.);

8.8. asmens duomenų saugojimo duomenų bazėje (-se) ir duomenų bazės (-ių) archyve terminas (-ai) ir veiksmai, kurie atliekami pasibaigus šiam terminui;

8.9. duomenų subjekto teisių įgyvendinimo tvarka;

8.10. asmens duomenų teikėjai ir gavėjai, asmens duomenų gavimo ir teikimo tvarka;

8.11. prieigos teisių ir įgaliojimų tvarkyti asmens duomenis suteikimo, naikinimo ir keitimo tvarka;

8.12. saugumo pažeidimų valdymo ir reagavimo į šiuos pažeidimus tvarka;

8.13. asmens duomenų kopijavimo, jei jis daromas, ir atkūrimo jų avarinio praradimo atvejais tvarka;

8.14. užtikrinamos techninės asmens duomenų saugumo priemonės;

8.15. kitos užtikrinamos asmens duomenų saugumo priemonės.

9. Bendrųjų reikalavimų 8 punkte nurodytas dokumentas (-ai) turi būti periodiškai, ne rečiau kaip kartą per 2 metus, peržiūrimas (-i) ir, reikalui esant, atnaujinamas (-i). Duomenų valdytojas turi vykdyti stebėseną ir kontrolę, kaip laikomasi šiame dokumente (-uose) įtvirtintų reikalavimų.

10. Jeigu yra paskirtas už duomenų apsaugą atsakingas asmuo, jis negali atlikti informacinės sistemos administratoriaus, t. y. asmens, prižiūrinčio informacinę sistemą ir (ar) jos infrastruktūrą, užtikrinančio jos veikimą ir elektroninės informacijos saugą, funkcijų.

11. Atsižvelgiant į saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, skiriami šie automatiniu būdu tvarkomų asmens duomenų saugumo lygiai, kur pirmasis saugumo lygis yra žemiausias, o trečiasis saugumo lygis yra aukščiausias:

11.1. pirmasis saugumo lygis – šiam saugumo lygiui priskirtas organizacines ir technines asmens duomenų saugumo priemones turi užtikrinti visi duomenų valdytojai ir duomenų tvarkytojai, tvarkantys viešai skelbiamus asmens duomenis, taip pat duomenų valdytojai ir duomenų tvarkytojai, automatiniu būdu tvarkantys asmens duomenis, prie kurių nėra prieigos per duomenų pardavimo tinklus, kurių nevaldo duomenų valdytojas ar duomenų tvarkytojas, (toliau – išoriniai duomenų perdavimo tinklai);

11.2. antrasis saugumo lygis – šiam saugumo lygiui priskirtas organizacines ir technines asmens duomenų saugumo priemones turi užtikrinti duomenų valdytojai ir duomenų tvarkytojai,

automatiniu būdu tvarkantys asmens duomenis, prie kurių yra prieiga per išorinius duomenų perdavimo tinklus;

11.3. trečiasis saugumo lygis – šiam saugumo lygiui priskirtas organizacines ir technines asmens duomenų saugumo priemones turi užtikrinti duomenų valdytojai ir duomenų tvarkytojai, automatiniu būdu tvarkantys ypatingus asmens duomenis.

12. Jeigu asmens duomenų tvarkymas atitinka kelis saugumo lygius, turi būti pasirenkamas aukštesnis saugumo lygis.

13. Siekiant užtikrinti pirmąjį saugumo lygį, turi būti įgyvendintos šios organizacinės ir techninės asmens duomenų saugumo priemonės:

13.1. užtikrinama prieigos prie asmens duomenų apsauga, valdymas ir kontrolė;

13.2. prieiga prie asmens duomenų gali būti suteikta tik tam asmeniui, kuriam asmens duomenys yra reikalingi jo funkcijoms vykdyti;

13.3. su asmens duomenimis galima atlikti tik tuos veiksmus, kuriems atlikti naudotojui yra suteiktos teisės;

13.4. prieigos prie asmens duomenų slaptažodžiai:

13.4.1. suteikiami, keičiami ir saugomi užtikrinant jų konfidencialumą;

13.4.2. unikalūs, sudaryti iš ne mažiau kaip 8 simbolių, nenaudojant asmeninio pobūdžio informacijos;

13.4.3. keičiami ne rečiau kaip kartą per 2 mėnesius;

13.4.4. pirmojo prisijungimo metu naudotojo privalomai keičiami;

13.5. užtikrinama asmens duomenų apsauga nuo neteisėto prisijungimo prie vidinio kompiuterinio tinklo elektroninių ryšių priemonėmis;

13.6. užtikrinamas patalpų, kuriose saugomi asmens duomenys, saugumas (apribojamas neįgaliotų asmenų patekimas į atitinkamas patalpas ir pan.);

13.7. užtikrinama kompiuterinės įrangos apsauga nuo kenksmingos programinės įrangos (antivirusinių programų įdiegimas, atnaujinimas ir pan.).

14. Siekiant užtikrinti antrąjį saugumo lygį, turi būti įgyvendintos pirmojo saugumo lygio organizacinės ir techninės asmens duomenų saugumo priemonės, nurodytos Bendrųjų reikalavimų 13 punkte, ir šios organizacinės ir techninės asmens duomenų saugumo priemonės:

14.1. kontroliuojama prieiga prie asmens duomenų tokiomis organizacinėmis ir techninėmis asmens duomenų saugumo priemonėmis, kurios fiksuoja ir kontroliuoja registravimosi bei teisių gavimo pastangas;

14.2. nustatomas leistinų nepavykusių prisijungimų prie programinės įrangos skaičius;

14.3. fiksuojami šie prisijungimų prie asmens duomenų įrašai: prisijungimo identifikatorius, data, laikas, trukmė, jungimosi rezultatas (sėkmingas, nesėkmingas). Šie įrašai turi būti saugomi ne trumpiau kaip 1 metus;

14.4. teikiamų asmens duomenų paieškos užklausoje nurodomas asmens duomenų naudojimo tikslas (-ai);

14.5. užtikrinamas saugių protokolų ir (arba) slaptažodžių naudojimas, kai asmens duomenys perduodami išoriniais duomenų perdavimo tinklais;

14.6. užtikrinama asmens duomenų, esančių išorinėse duomenų laikmenose ir elektroniniame pašte, saugos kontrolė ir ištrynimas po jų panaudojimo perkeliant į duomenų bazes ir pan.;

14.7. registruojami asmens duomenų kopijavimo, jei jis daromas, ir atkūrimo jų avarinio praradimo atveju veiksmai (kada ir kas atliko šiuos veiksmus);

14.8. užtikrinama, kad informacinių sistemų testavimas nebūtų vykdomas su realiais asmens duomenimis, išskyrus būtinus atvejus, kurių metu būtų naudojamos organizacinės ir techninės asmens duomenų saugumo priemonės, užtikrinančios realių asmens duomenų saugumą;

14.9. užtikrinamas patalpų, kuriose saugomi asmens duomenys, saugumas (užtikrinamas tik įgaliotų asmenų patekimas į atitinkamas patalpas ir pan.).

15. Siekiant užtikrinti trečiąjį saugumo lygį, turi būti įgyvendintos pirmojo ir antrojo saugumo lygio organizacinės ir techninės asmens duomenų saugumo priemonės, nurodytos

Bendrųjų reikalavimų 13 ir 14 punktuose, ir šios organizacinės ir techninės asmens duomenų saugumo priemonės:

15.1. fiksuojami prisijungimų prie asmens duomenų įrašai: bylos, prie kurių buvo jungtasi, atlikti veiksmai su asmens duomenimis (įvedimas, peržiūra, keitimas, naikinimas ir kiti asmens duomenų tvarkymo veiksmai). Šie įrašai turi būti saugomi ne trumpiau kaip 1 metus;

15.2. ne rečiau kaip kartą per 1 mėnesį peržiūrimas naudotojų prisijungimų prie duomenų bazės (-ių) įrašų elektroninis žurnalas ir duomenų valdytojui teikiamos peržiūros ataskaitos;

15.3. mobiliuosiuose įrenginiuose (nešiojamuosiuose kompiuteriuose, planšetėse, išmaniuosiuose telefonuose ir pan.), jeigu jie naudojami ne duomenų valdytojo ir (ar) duomenų tvarkytojo vidiniame kompiuterių tinkle, esantys ypatingi asmens duomenys ir prisijungimo prie duomenų valdytojo ir (ar) duomenų tvarkytojo tvarkomų asmens duomenų informacija šifruojama ar apsaugoma tokiomis priemonėmis, kurios atitiktų asmens duomenų atskleidimo keliamą riziką;

15.4. atsarginės asmens duomenų kopijos, jei jos daromos, saugomos kitoje patalpoje ar geografinėje vietoje negu aktyvi (veikianti) duomenų bazė;

15.5. šifruojami atsarginėse kopijose, archyvuose ir išorinėse duomenų laikmenose saugomi asmens duomenys;

15.6. šifruojami elektroniniu paštu perduodami ypatingi asmens duomenys.

16. Duomenų valdytojams ir duomenų tvarkytojams, tvarkantiems ypatingus asmens duomenis, atsižvelgiant į šių duomenų tvarkymo keliamą riziką, rekomenduojama įgyvendinti šias papildomas organizacines ir technines asmens duomenų saugumo priemones:

16.1. ne rečiau kaip kartą per 1 metus atlikti asmens duomenų tvarkymo rizikos vertinimą;

16.2. ne rečiau kaip kartą per 1 metus patikrinti avarinio asmens duomenų atkūrimo tvarką atliekant praktinius bandymus;

16.3. šifruoti aktyvioje (veikiančioje) duomenų bazėje saugomus asmens duomenis;

16.4. naudoti organizacines ir technines asmens duomenų saugumo priemones, kontroliuojančias duomenų bazę (-es), tarnybinę (-es) stotį (-is) ir informacinę sistemą administruojančių asmenų veiksmus.

## III. ASMENS DUOMENŲ TVARKYMAS NEAUTOMATINIU BŪDU SUSISTEMINTOSE RINKMENOSE

17. Neautomatiniu būdu tvarkant asmens duomenų susistemintas rinkmenas turi būti įgyvendintos šios organizacinės ir techninės asmens duomenų saugumo priemonės:

17.1. šios priemonės turi būti išdėstytos rašytinės (popierinės ar elektroninės) formos dokumente (duomenų valdytojo patvirtintose asmens duomenų tvarkymo taisyklėse, duomenų valdytojo ir duomenų tvarkytojo sudarytoje sutartyje ir pan.), kuriame nurodoma Bendrųjų reikalavimų 8.1–8.7, 8.9–8.10, ir 8.12–8.15 papunkčiuose nurodyta informacija, taip pat:

17.1.1. asmens duomenų saugojimo terminas (-ai) ir veiksmai, kurie atliekami pasibaigus šiam terminui;

17.1.2. įgaliojimų tvarkyti asmens duomenis suteikimo, naikinimo ir keitimo tvarka;

17.2. kontroliuojamas patekimas į patalpas, kuriose saugomi dokumentai ir jų archyvai.

18. Bendrųjų reikalavimų 17.1 papunktyje nurodytas dokumentas (-ai) turi būti periodiškai, ne rečiau kaip kartą per 2 metus, peržiūrimas (-i) ir, reikalui esant, atnaujinamas (-i). Duomenų valdytojas turi vykdyti stebėseną ir kontrolę, kaip laikomasi šiame dokumente (-uose) įtvirtintų reikalavimų.

## IV. BAIGIAMOSIOS NUOSTATOS

19. Duomenų valdytojas ir duomenų tvarkytojas, atsižvelgdamas į savo veiklos ypatumus (tarnybinės ir (arba) profesinės etikos reikalavimus ir pan.), saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, gali numatyti papildomas organizacines ir technines asmens duomenų saugumo priemones ir (arba) pasirinkti aukštesnį saugumo lygį.

20. Atsižvelgdama į naujų informacinių technologijų vystymąsi, Valstybinė duomenų apsaugos inspekcija rengia metodines rekomendacijas dėl taikytinų asmens duomenų saugumo priemonių.

21. Siekiant užtikrinti asmens duomenų saugumą, rekomenduojama vadovautis Lietuvos standartais LST ISO/IEC 27002, LST ISO/IEC 27001 ir kitais Lietuvos bei tarptautiniais standartais, reglamentuojančiais informacijos saugumą.

_____