Suvestinė redakcija nuo 2011-01-03 iki 2015-04-30

Įsakymas paskelbtas: Žin. 2008, Nr. 135-5298, i. k. 108110DISAK71(1.12)

VALSTYBINĖS DUOMENŲ APSAUGOS INSPEKCIJOS DIREKTORIAUS
Į S A K Y M A S

DĖL BENDRŲJŲ REIKALAVIMŲ ORGANIZACINĖMS IR TECHNINĖMS DUOMENŲ SAUGUMO PRIEMONĖMS PATVIRTINIMO

2008 m. lapkričio 12 d. Nr. 1T-71(1.12)
Vilnius

Įgyvendindamas Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (Žin., 1996, Nr. 63-1479; 2008, Nr. 22-804) 30 straipsnio 2 dalį:

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

2. N u s t a t a u, kad šis įsakymas įsigalioja 2009 m. sausio 1 d.

3. Neskelbiama.

DIREKTORIUS ALGIRDAS KUNČINAS

PATVIRTINTA
Valstybinės duomenų apsaugos
inspekcijos direktoriaus
2008 m. lapkričio 12 d.
įsakymu Nr. 1T-71(1.12)

BENDRIEJI REIKALAVIMAI ORGANIZACINĖMS IR TECHNINĖMS DUOMENŲ SAUGUMO PRIEMONĖMS

I. BENDROSIOS NUOSTATOS

1. Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms (toliau – Bendrieji reikalavimai) nustato bendruosius reikalavimus organizacinėms ir techninėms 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 (Žin., 1996, Nr. 63-1479; 2008, Nr. 22-804) 30 straipsniu.

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

4. Organizacinės ir techninės duomenų saugumo priemonės turi užtikrinti tokį saugumo lygį, kuris atitiktų saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, ir turi būti išdėstytos rašytinės formos dokumente (duomenų valdytojo patvirtintose asmens duomenų tvarkymo taisyklėse, duomenų valdytojo ir duomenų tvarkytojo sudarytoje sutartyje ir pan.).

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

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

II. DUOMENŲ TVARKYMAS AUTOMATINIU BŪDU

7. Atsižvelgiant į saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, skiriami šie automatiniu būdu tvarkomų asmens duomenų saugumo lygiai:

7.1. pirmasis saugumo lygis – šiam saugumo lygiui priskirtas organizacines ir technines duomenų saugumo priemones turi užtikrinti visi duomenų valdytojai, tvarkantys viešai skelbiamus asmens duomenis, taip pat duomenų valdytojai, automatiniu būdu tvarkantys asmens duomenis duomenų bazėje (-se), prie kurios (-ių) nėra prieigos per išorinius duomenų perdavimo tinklus;

7.2. antrasis saugumo lygis – šiam saugumo lygiui priskirtas organizacines ir technines duomenų saugumo priemones turi užtikrinti duomenų valdytojai, automatiniu būdu tvarkantys asmens duomenis duomenų bazėje (-se), prie kurios (-ių) yra prieiga per išorinius duomenų perdavimo tinklus, taip pat duomenų valdytojai, automatiniu būdu tvarkantys ypatingus asmens duomenis duomenų bazėje (-se), prie kurios (-ių) nėra prieigos per išorinius duomenų perdavimo tinklus;

7.3. trečiasis saugumo lygis – šiam saugumo lygiui priskirtas organizacines ir technines duomenų saugumo priemones turi užtikrinti duomenų valdytojai, automatiniu būdu tvarkantys ypatingus asmens duomenis duomenų bazėje (-se), prie kurios (-ių) yra prieiga per išorinius duomenų perdavimo tinklus.

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

9. Siekiant užtikrinti pirmąjį saugumo lygį, turi būti įgyvendintos šios organizacinės ir

techninės duomenų saugumo priemonės:

9.1. patvirtintas (-i) rašytinės formos dokumentas (-ai) (duomenų valdytojo patvirtintos asmens duomenų tvarkymo taisyklės, duomenų valdytojo ir duomenų tvarkytojo sudaryta sutartis ir pan.), kuriame (-iuose) turi būti nurodyta:

9.1.1. duomenų valdytojas;

9.1.2. duomenų tvarkytojai (jei tokie yra) ir jų atliekamos funkcijos;

9.1.3. teisės aktai ir standartai, kuriais vadovaujamasi tvarkant asmens duomenis;

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

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

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

9.1.7. asmens duomenų saugojimo aktyviojoje ir (ar) pasyviojoje duomenų bazėje (-se) terminas (-ai) ir veiksmai, kurie atliekami pasibaigus šiam terminui;

9.1.8. duomenų subjekto teisių įgyvendinimo tvarka;

9.1.9. asmens duomenų gavėjai ir asmens duomenų teikimo tvarka;

9.1.10. asmenų, kuriems suteikta teisė tvarkyti asmens duomenis, funkcijų paskirstymas;

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

9.1.12. asmenų, kuriems suteikta teisė tvarkyti asmens duomenis, informavimas ir apmokymų organizavimo tvarka;

9.1.13. asmens duomenų tvarkymo keliamos rizikos vertinimo atlikimo tvarka;

9.1.14. saugumo pažeidimų valdymas ir reagavimo į šiuos pažeidimus veiksmai;

9.1.15. duomenų atkūrimo jų avarinio praradimo atvejais tvarka;

9.1.16. periodiškas Bendrųjų reikalavimų 9.1 punkte nurodyto (-ų) dokumento (-ų) peržiūrėjimas (esant reikalui atnaujinimas) ir juose reglamentuotų nuostatų vykdymo kontrolė;

9.1.17. numatyta duomenų atsarginių kopijų darymo ir saugojimo tvarka;

9.1.18. reglamentuotos kitos užtikrinamos organizacinės ir techninės duomenų saugumo priemonės;

9.2. užtikrintas prieigos prie duomenų valdymas ir kontrolė:

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

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

9.2.3. užtikrintas slaptažodžių konfidencialumas juos suteikiant, pateikiant, reguliariai keičiant bei saugant, jeigu tapatybės patvirtinimas vykdomas naudojant slaptažodžius;

9.2.4. turi būti užtikrintos organizacinės ir techninės duomenų saugumo priemonės, skirtos apsaugoti duomenų bazes nuo neteisėto prisijungimo elektroninių ryšių priemonėmis;

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

9.4. užtikrinta kompiuterinės įrangos apsauga nuo žalingų programų (antivirusinių programų įdiegimas, atnaujinimas ir pan.).

10. Siekiant užtikrinti antrąjį saugumo lygį, turi būti įgyvendintos Bendrųjų reikalavimų 9 punkte numatytos organizacinės ir techninės duomenų saugumo priemonės bei šios organizacinės ir techninės duomenų saugumo priemonės:

10.1. jeigu yra paskirtas už duomenų apsaugą atsakingas asmuo ar padalinys, jis negali atlikti administratoriaus funkcijų;

10.2. kontroliuojama prieiga prie asmens duomenų tokiomis organizacinėmis ir

techninėmis duomenų saugumo priemonėmis, kurios fiksuoja ir kontroliuoja registravimosi bei teisių gavimo pastangas;

10.3. nustatytas leistinų nevykusių bandymų prisijungti prie duomenų bazės (-ių) skaičius;

10.4. fiksuojami šie asmenų, kuriems suteikta teisė tvarkyti asmens duomenis, prisijungimų prie duomenų bazės (-ių) įrašai: prisijungimo identifikatorius, data, laikas, trukmė, jungimosi rezultatas (sėkmingas, nesėkmingas), bylos, prie kurių buvo jungtasi, atlikti veiksmai su asmens duomenimis (įvedimas, peržiūra, keitimas, naikinimas ir kiti duomenų tvarkymo veiksmai). Šie įrašai turi būti saugomi ne trumpiau kaip 1 metus. Nesant galimybės užtikrinti šiame punkte numatytų priemonių techninėmis priemonėmis, jos turi būti užtikrintos organizacinėmis priemonėmis;

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

10.6. teikiamų asmens duomenų paieškos užklausoje turi būti suformuluotas duomenų paieškos tikslas (-ai);

10.7. užtikrinamas saugių protokolų ir (arba) slaptažodžių naudojimas, teikiant asmens duomenis išoriniais duomenų perdavimo tinklais;

10.8. užtikrintas išorinių duomenų laikmenų, kuriose saugomi gaunami ir teikiami asmens duomenys, registravimas, kontrolė ir asmens duomenų ištrynimas po jų panaudojimo perkeliant į duomenų bazes ir pan.;

10.9. registruojami avarinio asmens duomenų atkūrimo veiksmai (kada ir kas vykdė asmens duomenų atkūrimo veiksmus tiek automatiniu, tiek neautomatiniu būdu);

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

10.11. Nešiojamuosiuose kompiuteriuose, jeigu jie naudojami ne duomenų valdytojo vidiniame duomenų perdavimo tinkle, esantys asmens duomenys turi būti šifruojami tokiomis priemonėmis, kurios atitiktų duomenų tvarkymo keliamą riziką.

11. Siekiant užtikrinti trečiąjį saugumo lygį, turi būti įgyvendintos Bendrųjų reikalavimų 9 ir 10 punktuose numatytos organizacinės ir techninės duomenų saugumo priemonės bei šios organizacinės ir techninės duomenų saugumo priemonės:

11.1. šifruojami išorinėje duomenų laikmenoje teikiami asmens duomenys arba naudojamos saugos priemonės, užtikrinančios, kad asmens duomenys bus perduodami saugiai ir nebus galimybės tretiesiems asmenims jais pasinaudoti;

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

11.3. atsarginės asmens duomenų kopijos saugomos kitoje geografinėje vietoje negu aktyvi (veikianti) duomenų bazė;

11.4. šifruojami atsarginėse kopijose ir archyvuose saugomi asmens duomenys;

11.5. šifruojami išoriniais duomenų perdavimo tinklais perduodami asmens duomenys.

12. Duomenų valdytojams, tvarkantiems ypatingus asmens duomenis, kurių tvarkymas kelia didelę riziką, rekomenduojama įgyvendinti šias papildomas organizacines ir technines duomenų saugumo priemones:

12.1. ne rečiau kaip vieną kartą per metus atlikti asmens duomenų tvarkymo rizikos vertinimą;

12.2. ne rečiau kaip vieną kartą per dvejus metus atlikti asmens duomenų tvarkymo įgyvendintų organizacinių ir techninių saugumo priemonių įvertinimo auditą;

12.3. patikrinti avarinio asmens duomenų atkūrimo tvarką atliekant praktinius bandymus;

12.4. šifruoti aktyviose duomenų bazėse saugomus asmens duomenis;

12.5. naudoti organizacines ir technines duomenų saugumo priemones,

kontroliuojančias duomenų bazę (-es), tarnybinę (-es) stotį (-is) ir informacinę sistemą administruojančių asmenų veiksmus.

III. DUOMENŲ TVARKYMAS NEAUTOMATINIU BŪDU SUSISTEMINTOSE RINKMENOSE

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

13.1. patvirtintas (-i) rašytinės formos dokumentas (-ai) (asmens duomenų tvarkymo taisyklės, instrukcijos ir pan.), kuriame (-iuose) turi būti Bendrųjų reikalavimų 9.1.1–9.1.6, 9.1.8–9.1.10, 9.1.12–9.1.14, 9.1.16 ir 9.1.18 punktuose nurodyti reikalavimai, taip pat:

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

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

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

IV. BAIGIAMOSIOS NUOSTATOS

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

15. Siekiant užtikrinti asmens duomenų saugumą, rekomenduojama vadovautis Lietuvos standartais LST ISO/IEC 27002:2009, LST ISO/IEC 27001:2006 ir kitais Lietuvos bei tarptautiniais standartais, reglamentuojančiais informacijos saugumą.

Punkto pakeitimai:
Nr. 1T-80, 2010-10-01, Žin., 2010, Nr. 122-6246 (2010-10-14), i. k. 110110DISAK0001T-80

Pakeitimai:

1.
Valstybinė duomenų apsaugos inspekcija, Įsakymas
Nr. 1T-80, 2010-10-01, Žin., 2010, Nr. 122-6246 (2010-10-14), i. k. 110110DISAK0001T-80
Dėl Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymo Nr. 1T-71(1.12) "Dėl Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms patvirtinimo" pakeitimo