PERSONALOSKAITA

v.PS2018

BDAR

2018 m. gegužės 25 d. įsigaliojo Bendrasis duomenų apsaugos **reglamentas**, kuris skatina visas įmones ir organizacijas Lietuvoje bei ES stipriai peržiūrėti asmens duomenų saugos kultūrą.

PS BDAR'inėje versijoje (v.PS2018) realizuotos

tiek pagrindinės **BDAR prievolės**, tiek ir sudarytos visos sąlygos įgyvendinti **aukščiausio lygio asmens duomenų saugumą** ir prieigos prie jų valdymą, o įdiegti nauji programos plėtiniai užtikrins patogesnį ir saugesnį darbą su asmens duomenimis.

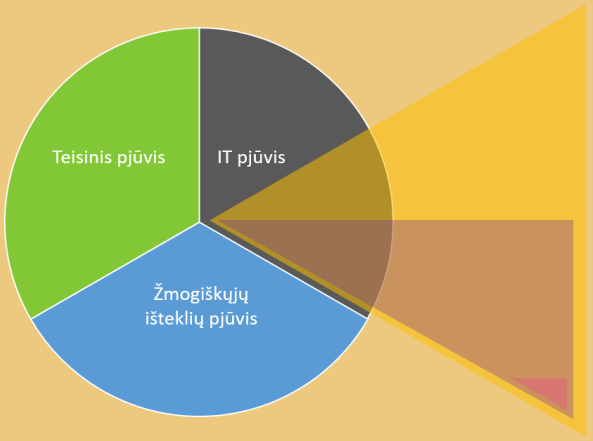
PS BDAR versijos diegimo ypatumai:

Vienkartinis naujos programos versijos diegimas yra atliekamas specialaus duomenų bazių konvertavimo įrankio pagalba, kuris slaptu algoritmu užkoduoja fizinių asmenų duomenis:

- Darbuotojų kortelės laukus: *vardas, pavardė, asmens kodas, darbuotojo nuotrauka, adresas, el. pašto adresas, tel. nr.*
- Šeimos narių laukus: *vardas, pavardė, asmens kodas.*
- Medicininės apžiūros informaciją: *diagnozė, išvados.*
- Mūsų asmenų laukus: *vardas, pavardė.*
- Partnerių laukus: *pavadinimas, ilgas pavadinimas, asmens/įmonės kodas.*

Fizinių asmenų duomenų kodavimas atliekamas kliento pasirinktu vienu iš trijų duomenų kodavimo lygiu: 2, 1 ar 0.

1 pav. Pasirengimas BDAR taikymui: 3 esminiai „PJŪVIAI“ ir BDAR reikalavimus įgyvendinantys duomenų kodavimo lygiai.



2 lygis. Duomenys koduojami individualiu „MasterKey“ raktu. **Aukščiausias duomenų saugumas.**

1 lygis. Duomenys koduojami universaliu raktu.

0 lygis. Duomenys šifruojami skaitmeniniu nekoduotu pavidalu.

Duomenų šifravimas **0 lygiu** sukurtas siekiant užtikrinti Jūsų turimos programos technologinį suderinamumą su naujomis versijomis, minimaliai kilstelėti duomenų saugumą, tačiau **nėra pakankamas įrodyti BDAR prievolių atitiktį.**

DUOMENŲ PRARADIMO RIZIKA

Galimos asmens duomenų praradimo situacijos ir apsaugos lygiai

RIZIKA PRARASTI DUOMENIS

DUOMENYS APSAUGOTI

7 ASMENS DUOMENŲ PRARADIMO SITUACIJOS:	0 DUOMENŲ APSAUGOS LYGIS Asmens duomenys saugomu skaitmeniniu nekoduotu pavidalu	1 DUOMENŲ APSAUGOS LYGIS Asmens duomenys saugomi universaliu raktu	2 DUOMENŲ APSAUGOS LYGIS Asmens duomenys saugomi individualiu „MasterKey“ raktu
Nors saugomi asmens duomenys yra šifruoti, juos galima lengvai atkoduoti. **(1)**	⚠	✓	✓
Bet kuris vartotojas gali prieiti prie PS duomenų bazėje (toliau, DB) esančių asmens duomenų. **(2)**	⚠	✓	✓
Skirtingi vartotojai prie programos jungiasi vienu ir tuo pačiu „SA“ (System Administrator“) vartotojo prisijungimu. **(3)**	⚠*	✓	✓
Nėra žinoma, kas ir kada jungėsi prie DB esančių asmens duomenų. **(4)**	⚠	✓	✓
DB esančius asmens duomenis galima pasiekti per Excel. **(5)**	⚠	✓	✓
DB esančius asmens duomenis galima nusikopijuoti ir perskaityti kitos įmonės kompiuteryje, kuriame suinstaliuota PS programa. **(6)**	⚠	⚠	✓
Nėra kaupiami ir saugomi vartotojų prisijungimai prie asmens duomenų. **(7)**	⚠	⚠**	⚠**

* Jei nėra „Vartotojų teisės“ modulio

** Jei nėra duomenų tvarkymo atsekamumo registro ir ataskaitos

Platesnis asmens duomenų praradimo atvejų aprašymas kitame puslapyje.

Duomenų praradimo rizika (1)

Nors saugomi asmens duomenys yra šifruoti, juos galima lengvai atkoduoti

Rizika pasirinkusiems 0 duomenų apsaugos lygį

Duomenų konvertavimas 0 lygiu išsaugo asmens duomenis skaitmeniniu nekoduotu pavidalu, tad įvykus duomenų vagystei (įmonės ofise arba išnešus ar perkėlus DB į kitą vietą), duomenys yra lengvai ir greitai nuskaitomi.

Duomenų praradimo rizika (2)

Bet kuris vartotojas gali prieiti prie PS programos DB esančių asmens duomenų.

Rizika pasirinkusiems 0 duomenų apsaugos lygį

Pasirinkus 0 apsaugos lygį, nėra galimybės valdyti asmens duomenų pasiekimo teisių vartotojams, vadinasi, bet kuris programos vartotojas, tiek buhalteris, vesdamas darbo užmokesčio apskaitą, tiek Prototechnikos konsultantas, atlikdamas programos atnaujinimų diegimą, ar IT administratorius gali matyti ir kitaip tvarkyti asmens duomenis.

Duomenų praradimo rizika (3)

Skirtingi vartotojai prie PS programos jungiasi vienu ir tuo pačiu „SA“ vartotojo prisijungimu

Rizika pasirinkusiems 0 duomenų apsaugos lygį be "Vartotojų teisės" modulio

Be "Vartotojų teisės" modulio nėra galimybės programoje kurti asmeninį prisijungimą turinčius vartotojus. Vadinasi, visi PS vartotojai jungiasi vienu ir tuo pačiu sisteminiu, o ne identifikuotu „SA“ vartotojo prisijungimu, turinčiu absoliučiai visas teises ir gali atlikti visus veiksmus SQL serveryje ir visose jame esančiose DB, įskaitant duomenų bazių kopijavimą ir serverio konfigūravimą.

Be "Vartotojų teisės" nežinosite, kuris asmuo priskirtas prie „SA“ vartotojo. „SA“ prisijungimas g. b. pririštas prie konkretaus Asmens iš Asmenų sąrašo, tuomet tiek buhalteris/-ė, tiek IT administratorius, tiek Prototechnikos konsultantas, jungdamasis su „SA“ slaptažodžiu, visus veiksmus atlieka nežinomo Asmens vardu.

Duomenų praradimo rizika (4)

Nėra žinoma, kas ir kada jungėsi prie DB esančių asmens duomenų

Rizika pasirinkusiems 0 duomenų apsaugos lygį

Kiekvienas prisijungimas prie DB esančių asmens duomenų yra atliekamas anonimiškai, t. y. nepaliekamas duomenis pasiekusio asmens „pėdsakas“, tad ir prieigos prie asmens duomenų žurnalas („Log'as“) nėra pildomas. Incidento atveju, nėra galimybės atpažinti, kas ir kada atliko neatitiktį su asmens duomenimis.

Duomenų praradimo rizika (5)

PS DB esančius asmens duomenis galima pasiekti per Excel

Rizika pasirinkusiems 0 duomenų apsaugos lygį

Be apribojimų prisijungti prie asmens duomenų galima ne tik per PS programą, bet ir per Excel, SQL Management Studio ar kitomis išorinėmis priemonėmis. Norintis pakenkti Asmuo, žinodamas neidentifikuotą „SA“ vartotojo slaptažodį, iš išorės gali „be pėdsakų“ lengvai ir greitai nutekinti tiek sąrašus, tiek duomenų bazių kopijas.

Duomenų praradimo rizika (6)

PS DB esančius asmens duomenis galima nusikopijuoti ir perskaityti kitos įmonės kompiuteryje, kuriame suinstaliuota ši programa

Rizika pasirinkusiems 1 duomenų apsaugos lygį

Įsigijus 1 lygio duomenų kodavimą būdą, DB esantys asmens duomenys užšifruojami universaliu raktu, kuris yra vienodas visiems mūsų PS programą turintiems klientams ir „įsiūtas“ į pačią programą. Vadinasi, paėmus DB kopiją ir pernešus ją į kitą kompiuterį, kuriame būtų suinstaliuota PS programa, duomenys būtų prieinami ir lengvai nuskaitomi svetimo kompiuterio „SA“ vartotojui, o su „SA“ vartotoju atsirastų galimybė valdyti vartotojus ir jų teises.

Duomenų praradimo rizika (7)

Nėra kaupiami ir saugomi vartotojų prisijungimai prie asmens duomenų

Rizika neturint duomenų tvarkymo registro ir ataskaitos.

Turintiems 1 ar 2 duomenų kodavimo būdą, prisijungimų prie asmens duomenų registras („Log'as“) pildomas tik nuo atsekamumo ataskaitos įsigijimo dienos. Jeigu ataskaita įsigyjama tik incidento atveju, ji bus tuščia, vadinasi, negalėsite įrodyti, kad duomenys Jūsų įmonėje tvarkomi teisėtai.

Kitame puslapyje sužinokite apie privalomas PS programos priemones, leidžiančias įgyvendinti esmines BDAR prievoles.

PRIVALOMOS PROGRAMOS PRIEMONĖS,

leidžiančios įgyvendinti esmines BDAR prievoles

PRIVALOMOS PRIEMONĖS

	Modulis „Vartotojų teisės“	Duomenų tvarkymo atsekamumas: registras, ataskaita	Duomenų kodavimas „MasterKey“ raktu (2 lygis)	Duomenų kodavimas universaliu raktu (1 lygis)	Periodinis vartotojų slaptažodžių keitimas	Ataskaita apie visus asmens duomenis programoje
Prievolė užtikrinti asmens duomenų saugumą. *Aktyvūs (darbiniai) duomenys.* BDAR IV sk., 2 skirsnis, 32 strp. III sk., 3 skirsnis, 17 str. >>>	+		+ (2 arba 1 lygis)		+	
Prievolė užtikrinti asmens duomenų saugumą. *Atsarginės duomenų kopijos.* BDAR IV sk., 2 skirsnis, 32 strp. III sk., 3 skirsnis, 17 str. >>>		+		+		+
Prievolė įrodyti, kad duomenys tvarkomi teisėtai. BDAR III sk., 1 skirsnis, 12 str. >>>	+	+	+	+		
Prievolė suteikti duomenų subjektui teisę susipažinti su duomenimis. BDAR I sk., 2 skirsnis, 15 str. >>>						+

PROTOTECHNIKA
- Sukurta Jūsų verslo augimui -

UAB PROTOTECHNIKA | info@prototechnika.lt | +370 5 2136774