

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

FUNDAMENTINIŲ MOKSLŲ FAKULTETAS

INFORMACINIŲ SISTEMŲ KATEDRA

Mantas Sebeika

**ĮMONĖS IT SISTEMŲ ATITIKIES BDAR VERTINIMAS IR AUTOMATIZUOTO ĮRANKIO KŪRIMAS**

**ASSESMENT OF IT SYSTEM COMPLIANCE TO GDPR AND TOOL DEVELOPMENT**

Baigiamasis bakalauro darbas

Programų inžinerija, valstybinis kodas 61209P109

Programų sistemų studijų kryptis

Vilnius, 2020

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

FUNDAMENTINIŲ MOKSLŲ FAKULTETAS

INFORMACINIŲ SISTEMŲ KATEDRA

TVIRTINU

Katedros vedėjas

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Parašas)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Vardas, pavardė)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Data)

Mantas Sebeika

**ĮMONĖS IT SISTEMŲ ATITIKIES BDAR VERTINIMAS IR AUTOMATIZUOTO ĮRANKIO KŪRIMAS**

**ASSESMENT OF IT SYSTEM COMPLIANCE TO GDPR AND TOOL DEVELOPMENT**

Baigiamasis bakalauro darbas

Programų inžinerijos studijų programa, valstybinis kodas 61209P109

Programų sistemų studijų kryptis

**Vadovas**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_

(Pedag. vardas, vardas, pavardė) (Parašas) (Data)

**Konsultantas**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

(Pedag. vardas, vardas, pavardė) (Parašas) (Data)

**Konsultantas**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

(Pedag. vardas, vardas, pavardė) (Parašas) (Data)

Vilnius, 2020

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Fundamentinių mokslų FAKULTETAS

INFORMACINIŲ SISTEMŲ KATEDRA

..........…....……………....studijų kryptis

.................………...…......studijų programa, valstybinis kodas ………………………..…specializacija

Informatika

TVIRTINU

Katedros vedėjas

Programų inžinerija

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Parašas)

Dalius Mažeika

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Vardas, pavardė)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Data)

**BAIGIAMOJO BAKALAURO DARBO (PROJEKTO)**

**UŽDUOTIS**

………........................Nr. ...............

Vilnius

Mantas Sebeika

Studentui (ei)...............…………................................….........................................................................…........…....  
 (Vardas, pavardė)

|  |
| --- |
| Įmonės IT sistemų atitikties BDAR vertinimas ir automatizuoto įrankio kūrimas |

Assesment of IT System Compliance to GDPAR and Tool Development

Baigiamojo darbo (projekto) tema: ......….........................................................................................................

........................................................................................................................................................................

patvirtinta 201…m. ………………..…… d. dekano potvarkiu Nr. ………….

Baigiamojo darbo (projekto) užbaigimo terminas 2019 m. birželio 1 d.

BAIGIAMOJO DARBO (PROJEKTO) UŽDUOTIS:

Duomenys: .................................................................................................................................……............................

..............................................................................................................................................................……..................

...................................................................................................................................................................…….............

Baigiamojo darbo uždaviniai:

* Atlikti IT saugos valdymo standartų ir metodikų analizę;
* Apžvelgti inforamcinių sistemų saugos audito metodikų analizę
* Suformuluoti reikalavimus įrankiui
* Atlikti įrankio projektavimą
* Pateikti audito išvadas

Aiškinamasis raštas: ..................................................................................................................................…….............

.......................................................................................................................................................................…….........

...................................................................................................................................................................…….............  
  
.......................................................................................................................................................................…….........

...................................................................................................................................................................…….............  
  
...............................................................................................................................................................…….................

Baigiamojo bakalauro darbo (projekto) konsultantai: …………………………………………………….…………..

................................................................................................................................................................……................  
 (Pareigos, vardas, pavardė)

Prof. dr. Dalius Mažeika

Vadovas ................................ ..........................................................  
 (Parašas) (Moksl. laipsnis, vardas, pavardė)

Užduotį gavau

…………………………………..

(Parašas)

Mantas Sebeika

..................................................

(Vardas, pavardė)

2019-10-15

2019-10-15

.......................................................

(Data)

Turinys

[ĮVADAS 8](#_Toc31010529)

[1. BDAR apžvalga 9](#_Toc31010530)

[1.1. Tvarkytojai ir valdytojai 12](#_Toc31010531)

[1.2. Duomenų apsaugos pareigūnas 13](#_Toc31010532)

[1.3. Duomenų tvarkymas 14](#_Toc31010533)

[2. BDAR atitikties vertinimo metodikos 16](#_Toc31010534)

[2.1. Valstybinės duomenų inspekcijos rekomendacijos 17](#_Toc31010535)

[3. IT audito metodika 23](#_Toc31010536)

[4. BDAR rekomenduojami sertifikatai 25](#_Toc31010537)

[5. Įrankiai užtikrinantys BDAR atitiktį 27](#_Toc31010538)

[6. Išvados 30](#_Toc31010539)

[Literatūros sąrašas 31](#_Toc31010540)

**Iliustracijų sąrašas**

[pav. 1 "Asmens duomenys" **Error! Bookmark not defined.**](file:///C:\Users\manta\Downloads\Baigiamasis%20Bakalaurinis%20Darbas%20Mantas%20Sebeika%20PRIF%2016_3%20DM%20komentarai%20(1).docx#_Toc31011015)

[pav. 2 "Asmens duomenų gyvavimo ciklas" 14](file:///C:\Users\manta\Downloads\Baigiamasis%20Bakalaurinis%20Darbas%20Mantas%20Sebeika%20PRIF%2016_3%20DM%20komentarai%20(1).docx#_Toc31011016)

[pav. 3 "Informacijos sauga" 17](file:///C:\Users\manta\Downloads\Baigiamasis%20Bakalaurinis%20Darbas%20Mantas%20Sebeika%20PRIF%2016_3%20DM%20komentarai%20(1).docx#_Toc31011017)

[pav. 4 "Standartų sąveika" 22](#_Toc31011018)

[pav. 5 "BDAR audito metodologija" 23](file:///C:\Users\manta\Downloads\Baigiamasis%20Bakalaurinis%20Darbas%20Mantas%20Sebeika%20PRIF%2016_3%20DM%20komentarai%20(1).docx#_Toc31011019)

[pav. 6 "Audito esminės sritys" 24](#_Toc31011020)

[pav. 7 "Įrankio "OneTrust" vartotojo sąsaja" 28](file:///C:\Users\manta\Downloads\Baigiamasis%20Bakalaurinis%20Darbas%20Mantas%20Sebeika%20PRIF%2016_3%20DM%20komentarai%20(1).docx#_Toc31011021)

[pav. 8 „Įrankio "Enablor" vartotojo sąsaja“ 29](#_Toc31011022)

**Lentelių sąrašas**

[lentelė 1 "Asmens duomenys" 9](#_Toc31011167)

[lentelė 2 "ISO Standartų koreliacija" 21](#_Toc31011168)

[lentelė 3 "Sertifikatų palyginimas" 25](#_Toc31011169)

[lentelė 4 "BDAR įrankių palyginimas" 29](#_Toc31011170)

**Santrumpos**

BDAR – Bendrasis duomenų apsaugos reglamentas;

GDPR – Bendrasis duomenų apsaugos reglamentas (angl. General data protection reglament);

DAP – Duomenų apsaugos pareigūnas;

KDV – Kompiuterinės darbo vietos;

VDAI – Valstybinė Duomenų apsaugos inspekcija;

DB - Duomenų bazė;

DBVS - Duomenų bazių valdymo sistema;

PS - Programų sistema;

PĮ - Programinė įranga;

IT - Informacinės technologijos;

IS - Informacinė sistema;

OS - Operacinė sistema;

ID – Identifikatorius;

EB – Europos Bendrija EN – anglų kalba ES – Europos Sąjunga; IEC – tarptautinė elektrotechnikos bendrija (angl. International Electrotechnical Commission);

ISO – tarptautinė standartizacijos organizacija (angl. International Organization for Standardization);

pav. – informacinis paveiklėlis.

# ĮVADAS

Europos Sąjungoje Bendrasis duomenų apsaugos reglamentas (angl. General data protection reglament) įsigaliojęs 2018 m. gegužės mėn. daro ženklią įtaką įmonių darbui su asmens duomenimis. Reglamento pagrindinis tikslas – sustiprinti asmens duomenų apsaugą, leisti piliečiams turėti kontrolę apie tai kas, kaip, ir kur naudoja jų duomenis. Juridiniams asmenims ir valstybės organizacijoms stipriai padidinta atsakomybė, priskirta naujų pareigų. Atsirado nauji techniniai (IT), organizaciniai ir procesiniai reikalavimai, galiausiai numatytos labai didelės (iki 4% metinės apyvartos) baudos už šių reikalavimų nesilaikymą. Verta paminėti, jog BDAR (angl. GDPR) galioja ne tik ES esančioms organizacijoms, bet ir įmonėms už ES ribų, kurios laiko ir/ar dirba su ES piliečių asmens duomenimis.

**Darbo aktualumas** - Bendrasis duomenų apsaugos reglamentas galioja jau beveik 2 metus, iki šiol nėra jo sertifikavimo standarto bei esminių taisyklių kaip reikėtų jo laikytis įmonėms. Dėl šios priežasties įmonėms labai sunku suprasti kaip tiksliai turi būti laikomasi šio reglamento ir kokie turi būti pagrindiniai punktai norint užtikrinti BDAR atitiktį įmonėje.

**Darbo tikslas** – Atlikti Bendrojo apsaugos reglamento atitikties įvertinimą įmonėje automatizuoto įrankio pagalba bei pateikti rekomendacijas pagal identifikuotas rizikas, remiantis ISO standartais ir VDAI rekomendacijomis.

Baigiamojo bakalaurinio darbo tikslui pasiekti iškelti tokie uždaviniai:

* Atlikti IT saugos valdymo standartų ir metodikų analizę;
* Apžvelgti informacinių sistemų saugos audito metodikų analizę;
* Suformuluoti reikalavimus įrankiui ;
* Atlikti įrankio projektavimą;
* Panaudojus sukurtą įrankį, atlikti įmonės atitikties BDAR vertinimą ir pateikti išvadas.

**Darbo praktinė vertė** – Bendrovei bus atliktas išsamus BDAR atitikties vertinimo projektas, kurio galutiniame rezultate bus pateiktos identifikuotos rizikos ir rekomendacijos kaip sumažinti rizikas arba jas pašalinti.

# BDAR apžvalga

Bendrasis duomenų apsaugos reglamentas yra nauja Europos duomenų apsaugos įstatymų sistema - ji pakeičia ankstesnę 1995 m. Duomenų apsaugos direktyvą. [1].

BDAR aprašomi išsamūs juridiniams asmenims taikomi asmens duomenų rinkimo, saugojimo ir valdymo reikalavimai. Būtina atkreipti dėmesį, jog reglamentas taikomas Europos organizacijoms, kurios tvarko asmens duomenis Europos Sąjungoje, ir už ES ribų veikiančioms organizacijoms, kurių veikloje yra renkami ar apdorojami ES gyventojų duomenys. [2].

BDAR taikomas, jeigu:

* Įmonė tvarko asmens duomenis ir yra įsisteigusi ES, nepaisant to, kur faktiškai tvarkomi asmens duomenys ir kokių piliečių asmens duomenys yra tvarkomi;
* Įmonė yra įsisteigusi už ES ribų, tačiau tvarko, stebi, apdoroja Europos sąjungos valstybių piliečių asmens duomenis.

Svarbu, jog Už ES ribų įsisteigusios įmonės, kurios tvarko ES piliečių duomenis, turi paskirti atstovą Europos Sąjungoje.

BDAR netaikomas, jeigu:

* duomenų subjektas yra miręs;
* duomenų subjektas yra juridinis asmuo;
* duomenis asmuo tvarko tikslais, nesusijusiais su jo vykdoma prekyba, verslu ar profesija.

Bendrajame duomenų apsaugo reglamente pagrindinė sąvoka yra asmens duomenis. Šiai sąvokai priskiriama bet kokia informacija apie asmenį, kurio tapatybė nustatyta arba gali būti nustatyta; toks asmuo dar vadinamas duomenų subjektu.

Asmens duomenų pagrindiniai tipai:

lentelė "Asmens duomenys"

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Identifikatoriai** | | | **Profiliavimo duomenys** | | | | | | **Stebėjimas** | |
| Asmens | Technologiniai | Biometriniai / Genetiniai | Netiesioginiai | Finansiniai | Socialiniai | Išoriniai | Sveikatos | Fiziniai | Vietos nusatymas | Video |

**Asmens duomenų tipų pavyzdžiai:**

**Asmens:**

* Vardas ir Pavardė;
* Asmens identifikavimo numeris/asmens kodas.

**Technologiniai:**

* IP adresas;
* Telelfono numeris;
* Elektroninio pašto adresas.

**Biometriniai / Genetiniai:**

* Pirštų antspaudai;
* Akies rainelė;
* Veido atpažinimas;
* Genetiniai tyrimai.

**Netiesioginiai:**

* Gyvenamosios vietos adresas;
* Automobilio valstybinis numeris;
* Gyvūnų/gyvulių identifikavimo numeris.

**Finansiniai:**

* Sąskaitos numeris;
* Kortelių numeris;
* Pinigų likutis sąskaitoje;
* Turima turtinė nuosavybė.

**Socialiniai:**

* Asmens profesniai duomenys (kvalifikacija, sertifikatai);
* Kriminalinė informacija;
* Religija;
* Šeimyninė padėtis ir šeimos sudėtis;
* Reputacija;
* Socialiniai ryšiai.

**Išoriniai:**

* Etniniai duomenys;
* Seksualinės orientacijos informacija;
* Pomėgiai.

**Sveikatos:**

* Medicinos duomenys (įskaitant istorinius);
* Tyrimų rezultatai;
* Fizinės negalios duomenys.

**Fiziniai:**

* Ūgis;
* Svoris;
* Amžius;
* Plaukų/odos spalva;
* Tatiuruotės;
* Lytis.

**Vietos nusatymas:**

* GPS informacija.

**Video:**

* Video atpažinimos (Vaizdinė medžiaga);
* Nuotraukos.

Specialių kategorijų asmens duomenų tvarkymas yra labai rizikingas, kadangi jie yra labai jautrūs fizinio asmens atžvilgiu. Norint rinkti šiuos duomenis privaloma turėti asmens sutikimą bei labai svarią bei pagrįsta priežastį. Šie duomenys turi būti techniškai apsaugoti nuo bet kokio duomenų nutekėjimo ar atskleidimo, jie turi aukščiausią prioritetą dėliojantis saugumo planus bei politikas įmonėje. [3]

Specialios duomenų kategorijos:

* rasinę arba etninę kilmę;
* lytinę orientaciją;
* politines pažiūras;
* religinius arba filosofinius įsitikinimus;
* narystę profesinėse sąjungose;
* genetinius, biometrinius ar sveikatos duomenis, išskyrus konkrečius atvejus (pvz., jeigu jums buvo duotas aiškus sutikimas arba jeigu asmens duomenis tvarkyti būtina dėl svarbių su viešuoju interesu susijusių priežasčių remiantis ES arba nacionaline teise);
* asmens duomenis, susijusius su apkaltinamaisiais nuosprendžiais ir nusikalstamomis veikomis, išskyrus atvejus, kai tai leidžiama pagal ES ar nacionalinę teisę.

# Tvarkytojai ir valdytojai

Tvarkymo metu asmens duomenys gali būti perduodami įvairioms skirtingoms įmonėms ar organizacijoms. Šiame cikle asmens duomenis tvarko du pagrindiniai pareigūnai:

* duomenų valdytojas, kuris priima sprendimą dėl asmens duomenų tvarkymo tikslo ir būdo;
* **A screenshot of a cell phone screen with text

  Description automatically generated**duomenų tvarkytojas, kuris saugo ir tvarko duomenis duomenų valdytojo vardu.

pav. 1 "Valdytojai ir tvarkytojai"

# Duomenų apsaugos pareigūnas

Duomenų apsaugos pareigūnas (DAP), kurį gali paskirti įmonė, privalo stebėti, kaip tvarkomi asmens duomenys, ir informuoti bei konsultuoti asmens duomenis tvarkančius darbuotojus apie jų pareigas. DAP taip pat bendradarbiauja su duomenų apsaugos institucija (DAI), kuri atlieka informacinio punkto funkciją DAI ir asmenų atžvilgiu.

Duomenų apsaugos pareigūno pagrindinės užduotys įmonėje:

* BDAR atitikties kontrolė organizacijos viduje;
* Aukštos duomenų apsaugos kultūros auginimas ir įtvirtinimas;
* Nešališkas rekomendavimas ir gerųjų praktikų rekomendavimas;
* Pagrindinias asmuo kontaktas VDAI;
* Pagrindinias asmuo kontaktas duomenų subjektams.

# Duomenų tvarkymas

Duomenų valdytojas gali naudotis tik duomenų tvarkytojo, kuris suteikia pakankamas garantijas, paslaugomis; šios garantijos turėtų būti įtrauktos į rašytinę susijusių šalių sutartį. Sutartyje taip pat turi būti nurodytos įvairios privalomos sąlygos, pavyzdžiui, kad duomenų tvarkytojas asmens duomenis tvarkys tik tuomet, kai tai jam nurodys duomenų valdytojas.

**Duomenų perdavimas už ES ribų**

Jeigu asmens duomenys perduodami už ES ribų, BDAR suteikiama apsauga turėtų „keliauti" kartu su duomenimis. Tai reiškia, kad jeigu eksportuojate duomenis į užsienį, jūsų įmonė privalo užtikrinti, kad būtų laikomasi vienos iš šių priemonių:

* ES nepriklausančios šalies apsaugos priemones ES laiko tinkamomis;
* Įmonė imasi būtinų priemonių, kad suteiktų tinkamas apsaugos priemones, pavyzdžiui, į sutartį, sudarytą su ne Europos asmens duomenų importuotoju, įtrauktų konkrečias sąlygas;
* A screenshot of a cell phone

  Description automatically generatedĮmonė remiasi konkrečiais perdavimo (išimties tvarka) pagrindais, pavyzdžiui, asmens sutikimu.

pav. "Asmens duomenų gyvavimo ciklas"

**Pagrindinės teisės, kurias įgavo asmuo:**

* **Teisė susipažinti (15 straipsnis)** – Duomenų subjektas turi teisę iš duomenų valdytojo gauti patvirtinimą, ar su juo susiję asmens duomenys yra tvarkomi, o jei tokie asmens duomenys yra tvarkomi, turi teisę susipažinti su jais.
* **Teisė reikalauti ištaisyti duomenis (16 straipsnis)** – Duomenų subjektas turi teisę reikalauti, kad duomanų valdytojas nepagrįstai nedelsdamas ištaisytų netikslius su juo susijusius asmens duomenis;
* **Teisė „būti pamirštam“ (17 straipsnis)** – Duomenų subjektas turi teisę reikalauti, kad duomanų valdytojas nepagrįstai nedelsdamas ištrintų su juo susijusius asmens duomenis, o duomenų valdytojas yra įpareigotas tai padaryti.
* **Teisė apriboti duomenų tvarkymą (18 straipsnis)** – Duomenų subjektas turi teisę reikalauti, kad duomanų valdytojas apribotų duomenų tvarkymą;
* **Teisė į duomenų perkeliamumą (20 straipsnis)** – Duomenų subjektas turi teisę gauti su juo susijusius asmens duomenis, kuriuos jis pateikė valdytojui susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu, ir turi teisę persiųsti tuos duomenis kitam duomenų valdytojui;
* **Teisė nesutikti (21 staripsnis)** – Duomenų subjektas turi teisę dėl su jo konkrečiu atveju susijusių priežaščių bet kuriuo metu nesutikti, kad su juo susiję asmens duomenys būtų tvarkomi.

Būtent dėl šių teisių įgavimo, informacinėms sistemoms, kurios yra diegiamos arba atnaujinamos iš pagrindų po BDAR įsigaliojimo, rekomenduojama turėti šiuos funkcionalumus:

* Galimybė atlikti asmens duomenų paiešką;
* Galimybė ištrinti duomenis automatinėmis priemonėmis;
* Galimybė klasifikuoti duomenis;
* Galimybė pažymėti duomenų laikymo trukmę.

Daugeliui Lietuvos įmonių tai pakankamai sudėtingos rekomendacijos, kadangi šių funkcionalumų įgyvendinimas senoms sistemoms gali būti neįmanomas arba labai sudėtingas ir kainuojantis didelius piniginius bei laiko kaštus. Informacinės sistemos keitimas į naujesnę yra brangus bei sukelia papildomų sunkumų įmonės viduje. [4].

# BDAR atitikties vertinimo metodikos

Nepaisant to, kad Bendrasis duomenų apsaugos reglamentas galioja jau beveik 2 metus, iki šiol nėra jo sertifikavimo standarto.

ES Bendrasis duomenų apsaugos reglamentas (GDPR) reikalauja organizacijas priimti tinkamas technines ir organizacines priemones - įskaitant politikas, procedūras ir procesus - apsaugoti asmens duomenis. Tarptautinis ISO 27001 standartas yra puikus atspirties taškas norint pasiekti techninius ir eksploatacinius reikalavimus, būtinus pažeidimų rizikai sumažinti. ISO 27701 patikslina reikalavimus Informacinėms saugumo valdymo sistemoms (ISVS), kurie yra grindžiami kontrolės tikslais, valdikliais, reikalavimais ir teikia rekomendacijas, kaip sukurti, įdiegti, prižiūrėti ir nuolat tobulinti ISVS (angl. PIMS). Organizacijos, įdiegusios ISO 27001, galės naudoti ISO 27701 standartą, kuris išplės Informacines saugumo valdymo sistemas (ISVS), kad jos apimtų privatumo valdymą, įskaitant duomenų tvarkymą. Įdiegę abu standartus, padėsite įvykdyti ir įrodyti, kad laikotės – BDAR (angl. GDPR) privatumo ir informacijos saugumo reikalavimų.

Bendrojo duomenų apsaugos reglamento 32 straipsnyje konkrečiai reikalaujama, kad organizacijos:

* Imtųsi priemonių pseudonimizuoti ir užšifruoti asmens duomenis;
* Užtikrinti nuolatinį sistemose esančių asmens duomenų konfidencialumą, vientisumą, prieinamumą ir atsparumą;
* Laiku atkurti prieinamumą prie asmens duomenų, jei įvyktų fizinis arba techninis incidentas;
* Įdiegti techninius ir organizacinius procesus, kurie užtikrintų duomenų tvarkymo saugumą, reguliarų tikrinimą ir įvertinimą.

pav. "Informacijos sauga"

**Informacijos sauga**

Konfidencialumas

Vientisumas

Prieinamumas

32 straipsnyje taip pat reikalaujama, kad būtų nustatyta ir sušvelninta rizika „dėl atsitiktinio ar neteisėto asmens duomenų sunaikinimo, praradimo, pakeitimo, neteisėto atskleidimo ar neteisėtos prieigos prie asmens duomenų“. ISO 27001 standartas atitinka visus aukščiau išvardytus reikalavimus.

BDAR 32 straipsnis yra pagrindinė nuostata, reikalaujanti techninių duomenų apsaugos priemonių. Nors jame pateikiami saugumo priemonių ir kontrolės pavyzdžiai, jame nėra išsamių nurodymų, ką reikia padaryti, kad tai pasiekti. Reglamentas verčia įmones atsižvelgti į esamą geriausią praktiką ir rekomendacijas, tokias kaip ISO 27001, kad sumažintų duomenų pažeidimo riziką. [5], [6], [7].

# Valstybinės duomenų inspekcijos rekomendacijos

Valstybinė duomenų apsaugos inspekcija (VDAI) Išleido „Tinkamų organizacinių ir techninių duomenų saugumo priemonių įgyvendinimo gaires asmens duomenų valdytojams ir tvarkytojams“. Gairėse rekomenduojama 20 minimalių organizacinių ir techninių duomenų saugumo reikalavimų, pakankamų tose organizacijose, kurių tvarkomų asmens duomenų saugumo rizika, susijusi su pavojais fizinių asmenų teisėms ir laisvėms, yra žema. Taigi, šiuos reikalavimus privalo įgyvendinti kiekviena asmens duomenis tvarkanti organizacija, o daugelis imtis ir papildomų priemonių, kad užtikrintų tinkamą tvarkomų asmens duomenų saugumą. Žemiau pateikiamas detalesnis aprašymas 10 minimalių techninių reikalavimų įmonėms.

1. **minimalių reikalavimų dėl tinkamų techninių duomenų saugumo priemonių**
2. **Prieigų kontrolė ir autentifikavimas.**

Privaloma įdiegti ir įgyvendinti Prieigų kontrolės sistema visiems IT sistemos naudotojams. Sistema turi leisti kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras. Turi būti vengiama naudoti bendras naudotojų paskyras. Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir slaptažodis. Prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiškumo lygio. Organizacija turi užtikrinti, kad visi darbuotojai būtų tinkamai informuoti apie IT sistemų saugumo kontrolę, susijusią su jų kasdieniu darbu. Darbuotojai, susiję su asmens duomenų tvarkymu, turi būti mokomi dėl atitinkamų duomenų apsaugos reikalavimų ir teisinių įsipareigojimų rengiant reguliarius mokymus, informavimo renginius ar instruktažus. Siūlomas mokymų dažnumas: kartą per metus.

1. **Techninių žurnalų įrašai ir stebėsena.**

Techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai, taikomajai programai, naudojamai asmens duomenų apdorojimui. Techniniuose žurnaluose turi būti matomi visi įmanomi prieigų prie asmens duomenų įrašų tipai (pvz., data, laikas, peržiūrėjimas, keitimas, panaikinimas). Siūlomas saugojimo terminas: ne mažiau kaip 6 mėnesiai. Techninių žurnalų įrašai turi turėti laiko žymas ir būti apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos. IT sistemose naudojami laiko apskaitos mechanizmai turi būti sinchronizuoti pagal bendrą laiko atskaitos šaltinį.

1. **Tarnybinių stočių, duomenų bazių apsauga.**

Duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų korektiškai ir naudotų atskirą paskyrą su priskirtomis žemiausiomis operacinės sistemos privilegijomis. Duomenų bazės ir taikomųjų programų tarnybinės stotys turi apdoroti tik tuos asmens duomenis, kurie yra reikalingi darbui, atitinkančiam duomenų apdorojimo tikslus.

1. **Darbo stočių apsauga.**

Naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti saugos nustatymų. Antivirusinės taikomosios programos ir jų informacijos apie virusus duomenų bazės turi būti atnaujinamos ne rečiau kaip kas savaitę. Naudotojams negalima turėti privilegijų diegti, šalinti, administruoti neautorizuotos programinės įrangos. IT sistemos turi turėti nustatytą sesijos laiką, t. y. naudotojui esant neaktyviam, neveiksniam sistemoje nustatytą laiką, jo sesija privalo būti nutraukta. Siūlomas neaktyvios sesijos laikas: ne daugiau kaip 15 min. Kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant.

1. **Tinklo ir komunikacijos sauga.**

Kai prieiga prie naudojamų IT sistemų yra vykdoma internetu, privaloma naudoti šifruotą komunikacijos kanalą, t. y. kriptografinius protokolus (pvz., TLS, SSL).

1. **Atsarginės kopijos.**

Atsarginės kopijos ir duomenų atstatymo procedūros privalo būti apibrėžtos, dokumentuotos ir aiškiai susaistytos su rolėmis ir pareigomis. Atsarginių kopijų laikmenoms privalo būti užtikrintas tinkamas fizinis aplinkos, patalpų saugos lygis, priklausantis nuo saugomų duomenų. Atsarginių kopijų darymo procesas turi būti stebimas, siekiant užtikrinti užbaigtumą, išsamumą. Pilnos atsarginės duomenų kopijos privalo būti daromos reguliariai. Siūlomas atsarginių kopijų darymo dažnumas: kasdien – pridedamoji kopija; kas savaitę – pilna kopija.

1. **Mobilieji, nešiojami įrenginiai.**

Mobiliųjų ir nešiojamų įrenginių administravimo procedūros privalo būti nustatytos ir dokumentuotos, aiškiai aprašant tinkamą tokių įrenginių naudojimąsi. Mobilieji, nešiojami įrenginiai, kuriais bus naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti. Mobilieji įrenginiai turi būti adekvataus prieigos kontrolės procedūrų lygio, kaip ir kita naudojama įranga asmens duomenims apdoroti.

1. **Programinės įrangos sauga.**

Informacinėse sistemose naudojama programinė įranga (asmens duomenims apdoroti) turi atitikti programinės įrangos saugos gerąją praktiką, programinės įrangos kūrimo struktūras, standartus. Specifiniai saugos reikalavimai turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose. Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos. Programinės įrangos kūrimo, testavimo ir verifikacijos etapai turi vykti atsižvelgiant į pagrindinius saugos reikalavimus.

1. **Duomenų naikinimas, šalinimas.**

Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinti visi joje esantys duomenys, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Tais atvejais, kai to padaryti neįmanoma (pvz., CD, DVD laikmenos ir pan.), turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti. Popierius ir nešiojamos duomenų laikmenos, kuriose buvo saugomi, kaupiami asmens duomenys, turi būti naikinami tam skirtais smulkintuvais.

1. **Fizinė sauga.**

Turi būti įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos.

Visa ši informacija aprašoma VDAI išleistose „Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams“ gairėse, kuriuose kiekvienas **techninių duomenų saugumo priemonių punktas yra aprašomas dar plačiau, pateikiant galimas rizikas.**

**Gairės yra** parengtos remiantis Europos Sąjungos kibernetinio saugumo agentūros (ENISA) rekomendacijomis („Handbook on Security of Personal Data Processing“, 2018 m.) ir ISO standartais LST EN ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“ bei LST EN ISO/IEC 27002:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“.

VDAI gairių punktai:

lentelė "ISO Standartų koreliacija"

|  |  |
| --- | --- |
| **VDAI gairių punktai BDAR atitikčiai** | **Atitikmuo ISO 27001:2017 A priede** |
| Prieigų kontrolė ir autentifikavimas | A.9 Prieigos valdymas |
| Techninių žurnalų įrašai ir stebėsena | A.12.4 Įvykių registravimas ir stebėsena |
| Tarnybinių stočių, duomenų bazių apsauga | A.12 Darbo saugumas |
| Darbo vietų apsauga | A.14.1 Informacinių sistemų saugumo reikalavimai |
| Tinklo ir komunikacijos sauga | A.13 Ryšių saugumas |
| Atsarginės kopijos | A.12.3 Atsarginės kopijos |
| Mobilieji, nešiojamieji įrenginiai | A.6.2 Mobilieji įrenginiai ir nuotolinis darbas |
| Programinės įrangos sauga | A.12.6 Techninio pažeidžiamumo valdymas  A.14.2 Kūrimo ir priežiūros procesų saugumas |
| Duomenų naikinimas, šalinimas | A.8.3.2 Duomenų laikmenų naikinimas  A.11.2.7 Saugus įrangos naikinimas arba pakartotinis naudojimas |
| Fizinė sauga | A.11 Fizinis ir aplinkos saugumas |

Visa tai įrodo, jog pagrindinis ir pirminis standartas, kuriuo organizacijos turėtu remtis bandant tvarkytis BDAR atitiktį yra ISO 27001 standartas. Šis standartas apima didžiąją dalį BDAR reikalavimų, todėl jis turėtų būti pagrindinė sudedamoji dali užtikrinant informacijos saugą įmonėje. [8]

Prie šio standarto galima jungti tokius standartus ir jų papildymus kaip ISO 29100:2011.

ISO / IEC 29100: 2011 pateikiama privatumo karkasą/metodologiją, kuri nurodo bendrą privatumo terminologiją:

* nusako veikėjus ir jų vaidmenis tvarkant asmenį identifikuojančią informaciją (angl. personally identifiable information);
* aprašomi privatumo apsaugos aspektai;
* pateikiamos nuorodos į žinomus informacinių technologijų privatumo principus.

ISO / IEC 29100: 2011 yra skirtas organizacijoms, užsiimančioms informacijos administravimu, priežiūra, specifikavimu, apdorojimu asmenį identifikuojančią informaciją. [9]

A screenshot of a cell phone

Description automatically generated

pav. "Standartų sąveika"

ISO/IEC 27701:2019 standartas apjungia dvi sritis – Saugos, kurios pagrindas yra ISO 27001 standartas ir privatumo, kurios pagrindas yra ISO 29100 standartas. ISO/IEC 27701:2019 standarte nurodomi reikalavimai ir nurodymai, kaip sukurti, įdiegti, prižiūrėti ir nuolat tobulinti Informacines saugumo valdymo sistemoms (ISVS), išplečiant ISO/IEC 27001 ir ISO / IEC 27002 standartus privatumo valdymui organizacijos kontekste. Standartas yra taikomas visų tipų ir dydžių organizacijoms, įskaitant valstybines ir privačias įmones, vyriausybės subjektus ir ne pelno siekiančias organizacijas, kurios yra asmens duomenų valdytojai ir tvarkytojai. [10].

Įsidiegus ir realizavus aptartus standartus galima teigti, jog organizaciją pilnai atitinką BDAR reikalavimus ir yra sumažinus visas rizikas susijusias su asmens duomenimis. [11].

# IT audito metodika

Audituojant arba atliekant atitiktį labai svarbu laikytis plano ir sekti užsibrėžtų metodų. Atitikties įvertinimo metu neužtenka žinoti auditavimo srities ir ją gerai išmanyti, būtina mokėti auditavimo metodologiją ir pagrindinius punktus, kurie leistų auditą paversti sklandžiu procesu.

pav. "BDAR audito metodologija"

Šeši pagrindiniai punktai audito ataskaitai yra:

1. Formaliai pateikti audito rezultatai, audito klientui;
2. Pateikti formalų audito baigties rezultatą;
3. Pateikti konkrečias sritis, kuriose reikia taisomųjų veiksmų. Taip pat pateikti rekomendacijas taisytinoms sritims;
4. Ataskaitą pateikti kaip naudingą šaltinį visoms visoms šalims tiriančioms audito subjektą ar audito temą;
5. Naudoti kaip tolimesnio audito pagrindą, jei audito išvados buvo pateiktos;
6. Skatinti audito patikimumą bei naudojimą, kai jis gerai išvystytas ir pateiktas.

Pasiruošimas

Rašymas

Pabaigimas

Pradžia

Pabaiga

Kiti svartymai

* Audito tikslai
* Ataskaitos vertė
* IS audito ataskaitų tipai
* Ataskaitos naudotojų identifikavimas
* Audito standartų atitiktis
* Teisinių reikalavimų atitiktis
* Pranešimas apie nelegalios ar apgaulingos veiklos galimybę
* Atskirų konfidencialių ataskaitų naudojimas
* Bendravimo veiksniai
* Ilgis ir turinys
* IS audito ataskaitos turinys
* IS auditos ataskaitos šablonas
* Ataskaitos rengimo procesas
* Pridedama papildoma informacija
* Galutinis redagavimas, peržiūra ir patvirtinimas
* Ataskaitos atidavimas klientui

pav. "Audito esminės sritys"

**Pirmas etapas - pasiruošimas rašyti**

Pirmame etape, ruošiantis rašyti, pagrindinis dėmesys skiriamas turinio reikalavimams. Jie grindžiami audito tipu ir užduoties logika, audito dalyko sudėtingumu, audito standartai ir gairėmis, skaitytojų auditorija. Pirmasis etapas taip pat apima ataskaitos struktūros nustatymą, atsižvelgiant į numatomą ataskaitos ilgį. Gali būti pateikiama santrauka, turinio lentelė ar priedai jei jie yra reikalingi. Jei įmonės audito organizacija jau yra nustačiusi ataskaitos struktūrą, metmenis ar šabloną tai yra įtraukta į šias instrukcijas kadangi, tai auditoriui gali padėti atlikti rašymo procesą. Pirmojo etapo metu gali būti įterptos tam tikros detalės pavyzdžiui: audito subjektas, audito pavadinimas, audito užduoties numeris ir audito laikotarpis į ataskaitos šabloną.

**Antrasis etapas - ataskaitos rašymas**

Ataskaitos rašymo etape pateikiama konkreti informacija apie audito apimtį, tikslus, metodiką, išvadas. Rekomendacijos ištraukiamos iš audito darbo dokumentų ir įterpiamos į ataskaitos šabloną. Didžioji pranešimo dalis, tekstas, taip pat rašomas šioje fazėje. Metodiką reikia sutrumpinti iki konkretaus paaiškinimo kaip buvo atliktas auditas. Taip pat gali reikėti parašyti ataskaitos įvadą ir santrauką, audito rezultatai turi būti parašyti arba perrašyti, kad būtų įtraukta tinkamas išvadų formatas. Šio etapo rezultatas yra oficialus ataskaitos projektas, kuris gali būti pateiktas klientų peržiūrai, atsiliepimams ir vadovybės atsakymui gauti.

**Trečias etapas - ataskaitos baigimas**

Ataskaitos baigimo etapas parengia galutinę audito ataskaitą, kad ji būtų pateikta klientui ir visiems kitiems paskirtiems asmenims. Audito valdymo atsakymai įterpiami į ataskaitą su galimybe, kad auditorius komentuos bei darys galutinius pakeitimus. [12].

# BDAR rekomenduojami sertifikatai

Kokybiškas auditas arba atitikties įvertinimas reikalauja patirties ir aukšto kvalifikacijos lygio. Norint įvertinti sistemą ar organizacijos atitiktį tam tikram reikalavimui, dažniausiai prašoma įrodyti savo kvalifikacijos lygi. Bendrasis duomenų apsaugos reglamentas reikalauja ne tik teisinių, bet ir informacinių technologinių žinių. Vienas iš būdų kaip pasiekti aukšta kvalifikacijos lygį yra sertifikatų išlaikymas ir jų pritaikymas praktikoje. Norint atlikti kokybišką BDAR atitiktį, rekomenduojamas CIPP/E sertifikatas, kuris puikiai tinka Duomenų apsaugos pareigūnams (DPO). Šis sertifikatas yra puikus įvadas į BDAR ir šio reglamento specifikaciją. Prie šio sertifikato galima pridėti ir CIPM, kuris apžvelgia Privatumo valdymą organizacijoje. Kadangi Bendrajame duomenų apsaugos reglamente nemažai šnekama apie technologinius procesus ir sprendimus, CIPT sertifikatas būtinas norint užtikrinti techninę BDAR atitiktį įmonėje. [13].

lentelė "Sertifikatų palyginimas"

|  |  |  |
| --- | --- | --- |
| A close up of a sign  Description automatically generated | A close up of a sign  Description automatically generated | A picture containing gambling house, pool ball, room  Description automatically generated |
| Mokomoji medžiaga | Mokomoji medžiaga | Mokomoji medžiaga |
| * Kaip susikurti įmonės viziją * Kaip sudaryti privatumo komandą įmonėje * Kaip sukurti ir įgyvendinti privatumo programos pagrindus * Kaip bendrauti su suinteresuotosiomis šalimis * Kaip įvertinti našumą * Privatumo programos gyvavimo ciklas | * Įvadas į Europos duomenų apsaugą * Europos reguliavimo institucijos * Teisinė bazė * Europos duomenų apsaugos įstatymų ir taisyklių laikymasis * Tarptautinis duomenų perdavimas | * Kritinės duomenų apsaugos koncepcijos ir praktika, darančios įtaką IT * Vartotojų duomenų apsaugos lūkesčiai ir atsakomybė * Kaip pakeisti privatumą ankstyvose IT produktų ir paslaugų stadijose, kad būtų galima kontroliuoti kaštus, tikslumą ir greitį rinkoje * Kaip pritaikyti duomenų apsaugos praktiką renkant ir perduodant duomenis * Kaip iš anksto numatyti duomenų apsaugą daiktų internetui (angl. Internet of Things – IoT) * Kaip duomenų apsaugą įtraukti į duomenų klasifikavimą ir tokias naujas technologijas kaip debesų kompiuterija, veido atpažinimą ir stebėjimą * Kaip komunikuoti su partneriais dėl klausimų susijusiu su duomenų apsauga |

**CIPP/E** - Skirtas pradedantiesiems gilintis į BDAR ir jį pradėti įgyvendinti savo įmonėje nuo pradmenų. Nuo šio sertifikato reikėtų pradėti, jei yra poreikis išsilaikyti visus paminėtus sertifikatus. CIPP/E rekomenduotinas tokioms specialybėms:

* Duomenų apsaugos pareigūnams;
* Duomenų apsaugos teisininkams;
* Duomenų įrašų tvarkytojams;
* Žmogiškųjų išteklių skyriaus vadovams;
* Kiekvienam asmeniui, kuris naudoja, tvarko ir prižiūri asmens duomenis;

**CIPM** – Labiausiai aktualus vadybininkams ir Duomenų apsaugos pareigūnams, kurie atsakingi už saugumo ir privatumo įgyvendinimą įmonėje. Aukštesnė CIPP/E pakopą, dažnai galima šiuos sertifikatus laikyti vienu metu. CIPM rekomenduotinas tokioms specialybėms:

* Duomenų apsaugos pareigūnams;
* Teisinės atitikties pareigūnams
* Auditoriams;
* Saugumo vadybininkams;
* Informacijos valdytojams;
* Bet kuris asmuo, susijęs su duomenų apsaugos procesais ir moduliais. [14].

**CIPT** – IT specialistams, kurie nori sugebėti nuo pat pradžių sukurti organizacijos duomenų apsaugos struktūrą ir modelį. Daugiausiai techninių žinių reikalaujantis sertifikatas. CIPT rekomenduotinas tokioms specialybėms:

* Duomenų apsaugos pareigūnams;
* IT vadovams ir administratoriams;
* Duomenų įrašų tvarkytojams;
* Sistemų kūrėjams;
* IT saugumo specialistams;
* Kiekvienam, kuriančiam IT sistemas.

Visi lyginami sertifikatai moko kaip įmonėje užtikrinti saugumo bei privatumo modelius, būtent apie tai yra BDAR. Rekomenduotina įmonėje turėti žmones, kurie turi šiuos sertifikatus, nesvarbu ar tai būtų vienas žmogus ar pavieniai asmenys. [15].

# Įrankiai užtikrinantys BDAR atitiktį

Įmonėje labai svarbu mokėti valdyti resursus ir juos mažinti, kad darbas būtų efektyvesnis ir produktyvesnis. Auditavimas arba atitikties vertinimas dažniausiai užima labai daug laiko ir žmogiškųjų resursų, kadangi reikia susirinkti didelį kiekį informacijos ir ją susisteminti. BDAR atitikties vertinimas ne išimtis, kadangi profesionaliai atlikti įmonės įvertinimą, reikia susipažinti su visa įmonės IT architektūra ir infrastruktūra. Norint sumažinti šiuos kaštus reikalingas proceso automatizavimas. Automatizuotų įrankių, kurie padėtų spręsti BDAR atitikties problemas nėra daug, kadangi reglamentas gyvuoja dar tik nepilnus 2 metus.

Vienas labiausiai paplitusių ir žinomiausių įrankių rinkoje yra „OneTrust“. Šis įrankis turi automatizuota atitikties įvertinimo modulį, kurio pagalbą, užpildžius esantį klausimyną įrankyje, nustatyti įmonės rizikas pagal BDAR ir ISO 97000 standartus. Taip pat automatizuotas atitikties įvertinimo modulis savyje turi Poveikio duomenų apsaugai vertinimo (PDAV) šabloną, kurio pagalbą galimą nustatyti rizikas informacinėms sistemoms, kurios savyje turi didelį kiekį didelės rizikos asmens duomenų. [16]

A screenshot of a cell phone

Description automatically generated

pav. "Įrankio "OneTrust" vartotojo sąsaja"

Organizacijoje, kurioje vartojama tik Lietuvių kalba, taip pat yra sprendimas. Įrankis „Enablor“, kuris taip pat padeda organizacijose užtikrinti BDAR, turi Lietuvišką pilną lietuvių kalbos vertimą. Šis įrankis skirtas vertinti organizacijos saugumo bei privatumo rizikas, jas valdyti ir pateikti sprendimus. „Enablor“ puikiai tinka ir Duomenų apsaugos pareigūnams, kurie nori automatizuoti rizikų vertinimą, sutikimų surinkimą bei sudarinėti duomenų žemėlapius. [17]

pav. „Įrankio "Enablor" vartotojo sąsaja“A screenshot of a cell phone

Description automatically generated

lentelė "BDAR įrankių palyginimas"

|  |  |  |
| --- | --- | --- |
| **Platforma/Įrankis**  **Kategorija** | **„Onetrust“** | **„Enablor“** |
| **Tinkamumas** | Tinka didelėms įmonės su nedaug organizacinių vienetų | Tinka mažoms ir vidutinio tipo įmonėms |
| **Kalbos** | Daugiau nei 100 kalbų, tačiau nėra Lietuvių kalbos. | * Danų kalba * Švedų kalba * Norvegų kalba * Anglų kalba * Lietuvių kalba |
| **Platformos tipas** | SaaS – Programinė įranga kaip paslauga (angl. software as a service) | SaaS – Programinė įranga kaip paslauga (angl. software as a service) |
| **Pagalba (angl. support)** | 24/7 Interaktyvi pagalba | Interaktyvi pagalba tik darbo valandomis |
| **Nemokama versija** | 14 dienų nemokama versija | Nėra |
| **Platformos naudojimo mokymai** | * Dokumentacija * Tiesiogiai vykdomi/transliuojami mokymai * Internetiniai seminarai * Asmeniškai | * Dokumentacija * Asmeniškai |
| **Kaina** | Konkreti kaina nėra nežinoma, ji susideda iš daug modulių. Dėl kainos kreipiamasi tiesiogiai į „Onetrust“. | Konkreti kaina nėra nežinoma. Kaina derinama tiesiogiai su „Enablor“ atstovais. |

Abu lyginami įrankiai yra tikrai išvystiti ir turi daug modulių, kurie gali padėti organizacijoje gerinti BDAR atitiktį, tačiau pagrindinis minusas yra, jog šie įrankiai negali pasiūlyti atskiro vieno modulio. Mažesnėms įmonėms tai yra labai svarbu, kadangi visas įrankis mažoms įmonėms yra pare didelis t.y. perkant įranki sumokami pakankamai dideli pinigai, tačiau dalis funkcionalumų yra nenaudojami.

# Išvados

Organizacijoje užtikrinti Bendrojo duomenų reglamento atitiktį neužtenka turėti teisinių bei technologinių žinių. Kadangi BDAR skatinama atsižvelgti į naujausias tendencijas ir praktikas, visi dokumentai bei parinkti auditai turi būti peržvelgiami bent į metus kartą, taip užtikrinant minimalias rizikas įmonėje. BDAR susideda iš didelio kiekio saugumo bei privatumo metodikų ir tai įneša į rinką šiek tiek sąmyšio. Dėl šių priežasčių įmonės siunčia darbuotojus laikytis sertifikatus, diegiasi įrankius, kurie padeda turėti naujausias žinias apie BDAR ir maksimaliai sumažina galimas rizikas.

Atitikties įvertinimas įmonėse atneša daug atsakomybės auditoriui, kadangi neaprašęs visų galimų rizikų, jis gali likti atsakinga už nutikusius pažeidimus. Atitikties įvertintojai privalo išmanyti naujausias tendencijas, taikyti atitinkamus standartus bei dirbti pagal išmoktą ir pasitvirtintą metodiką, kad darbo rezultatas būtų aukščiausios kokybės ir atneštu pridėtinės vertės audituojamai įmonei.

# Literatūros sąrašas

1. Kas yra BDAR ? 2019.01.21. Interneto prieiga <https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018>
2. Duomenų apsauga pagal BDAR. 2019-10-14. Interneto prieiga <https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_lt.htm#shortcut-0>
3. Bendrasis duomenų apsaugos reglamentas. 2 skyrius. 5-11 straipsnis. Interneto prieiga. <https://gdpr.algolia.com/lt/gdpr-article-9>
4. 10 pagrindinių BDAR reikalavimų. 2018.10.02. Internetin4 prieiga. <https://advisera.com/eugdpracademy/knowledgebase/a-summary-of-10-key-gdpr-requirements/>
5. ISO standartų koreliacija su BDAR. Internetinė prieiga <https://www.itgovernance.co.uk/gdpr-and-iso-27001>
6. ISO 29000 standartas. Internetinė prieiga <https://pecb.com/whitepaper/iso-29100--how-can-organizations-secure-its-privacy-network>
7. (ENISA) rekomendacijomis („Handbook on Security of Personal Data Processing“, 2018 m.)
8. VDAI saugumo priemonių gairės. 2019-12-18. Internetinė prieiga. <https://vdai.lrv.lt/uploads/vdai/documents/files/VDAI_saugumo_priemoniu_gaires-2019-12-18.pdf> -
9. ISO 29000 standartas. Internetinė prieiga <https://www.iso.org/standard/45123.html>
10. ISO 27701 standartas. Internetinė prieiga <https://www.iso.org/standard/71670.html>
11. „Data Protection Certification Mechanisms“ Study on Articles 42 and 43 of the Regulation (EU) 2016/679 <https://ec.europa.eu/info/sites/info/files/certification_study_annexes_publish.pdf>
12. „Information Systems Auditing: Tools and Techniques“, 2015, ISACA
13. „Data Protection Officer (DPO) Training Bundle Official IAPP Training and Certification” <https://www2.deloitte.com/content/dam/Deloitte/ro/Documents/risk/DPO%20Training%20Bundle%20Brochure_Deloitte%20Academy.pdf>
14. Sertifikatai CIPP/E ir CIPM. Internetinė prieiga <https://iapp.org/certify/cippe-cipm/>
15. Sertifikatai CIPT. Internetinė prieiga <https://iapp.org/certify/cipt/>
16. Įrankis „OneTrust“. Internetinė prieiga <https://www.onetrust.com/>
17. Įrankis „Enablor“. Internetinė prieiga <http://www.itrusta.lt/>