

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 duomenų gyvavimo ciklas" 14](file:///C:\Users\manta\Desktop\Mokslai\Bakalauras\Bakalauras\Rašliava\Baigiamasis%20Bakalaurinis%20Darbas%20Mantas%20Sebeika%20PRIF%2016_3%20v.2.docx#_Toc40019690)

[pav. 2 "Informacijos sauga" 17](file:///C:\Users\manta\Desktop\Mokslai\Bakalauras\Bakalauras\Rašliava\Baigiamasis%20Bakalaurinis%20Darbas%20Mantas%20Sebeika%20PRIF%2016_3%20v.2.docx#_Toc40019691)

[pav. 3 "Standartų sąveika" 22](#_Toc40019692)

[pav. 4 "BDAR audito metodologija" 23](file:///C:\Users\manta\Desktop\Mokslai\Bakalauras\Bakalauras\Rašliava\Baigiamasis%20Bakalaurinis%20Darbas%20Mantas%20Sebeika%20PRIF%2016_3%20v.2.docx#_Toc40019693)

[pav. 5 "Audito esminės sritys" 24](#_Toc40019694)

[pav. 6 "Įrankio "OneTrust" vartotojo sąsaja" 28](file:///C:\Users\manta\Desktop\Mokslai\Bakalauras\Bakalauras\Rašliava\Baigiamasis%20Bakalaurinis%20Darbas%20Mantas%20Sebeika%20PRIF%2016_3%20v.2.docx#_Toc40019695)

[pav. 7 „Įrankio "Enablor" vartotojo sąsaja“ 29](#_Toc40019696)

**Lentelių sąrašas**

[lentelė 1 "Asmens duomenys" 9](#_Toc40019699)

[lentelė 2 "ISO Standartų koreliacija" 21](#_Toc40019700)

[lentelė 3 "Sertifikatų palyginimas" 25](#_Toc40019701)

[lentelė 4 "BDAR įrankių palyginimas" 29](#_Toc40019702)

**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 1 "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. 1 "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. 2 "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 2 "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. 3 "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. 4 "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. 5 "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 3 "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. 6 "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. 7 „Įrankio "Enablor" vartotojo sąsaja“A screenshot of a cell phone

Description automatically generated

lentelė 4 "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.

# Poreikių specifikacija

# Pradinė verslo analizė

### Esamos būsenos analizė

Įsigaliojus Bendrąjąm duomenų apsaugos reglamentui (toliau BDAR), Valstybinė duomenų apsaugos inspekcija (toliau VDAI) paruošė gairės, pagal kurias įmonė privalo įsisvertinti ar atitinka pagrindines reglamento nuostatas ir taip nepažeidžia Europos sąjungoje įsigaliojusio reglamento

Dėl šios priežasties įmonės privalo įsivertinti savo veiklos bei IT infrastruktūros atitiktį vadovaujanti pateiktomis Valstybinės duomenų apsaugos gairėmis. Vienas iš lengviausių ir greičiausių būdų tai padaryti yra užpildyti IT infrastruktūros klausimyna sudaryta pagal ISO saugos standartus bei VDAI gaires. Kadangi įmonė turi turėti įrodymą, jog ji atitinka visus BDAR reikalavimus, atitikties įvertinimui dažniausiai yra paskiriamas įmonės darbuotojas atsakingas už duomenų apsaugą, kuri yra vadinamas duomenų aspaugos pareigūnų (DAP), arba įmonė samdosi išorinį duomenų apsaugos pareigūna, kuris įvertinima atlieka ir pateikia išvadas

Pagrindinė IT atitikties dalis yra IT klausimynas, kuris dažnu atveju įmonei duodamas užpildyti popieriniu arba excel formatu. Šis klausimyno užpildymo būdas sukelia daug probleminių sričių, tokių kaip: klausimyno perdavimas ir gavimas, klausimyno metodologijos nutekėjimas tretiems asmenimis, didelis laiko išteklių sunaudojimas.

Dažnu atveju vienas darbuotojas negali atsakyti į visus IT klausimyne pateiktus klausimus, todėl klausimynas perduodamas arba siunčiamas kitam darbuotojui. Šiuo atveju yra sunaudojamas papildomas laikas ir dažmu atveju atsiranda vis daugiau klausimyno kopijų, kadangi kiekvienas darbuotojas daro vis kitokius pakeitimus. Taip klausimyno pildymas užtrunka ilgai ir darbas dažnai būna atliktas nekorektiškai su dideliais informacijos netikslumais

A close up of a map

Description automatically generated

pav. 1 Vaizdusis paveikslėlis -Esama sistema

“IT klausimynas” sistemoje galima rasite informaciją, susijusią su grupės korporatyviniais standartais, tinklapyje pagal poreikį galimą įkelti dokumentus bei mokymus skirtus skaityti įmonės darbuotojams. Tinklapyje yra galimybė atlikti žinių patikrinimo testus susijusius su Bendruoju duomenų apsaugos reglamentu, taip pat galima pateikti klausimus ar užklausas įmonės duomenų apsaugos pareigūnui.

Duomenų apsaugos pareigūnas turi paruošti reikiama medžiaga, kuri būtu keliama į sistema kaip mokomoji medžiaga ir specifikuotas testas.

Darbuotojas turi prisijungti į įmonei sukurtą „GDPR Partners“ sistemą su savo įmonės el.paštu, kad jis būtų autorizuotas sistemoje. Po sėkmingo prisijungimo darbuotojas turi susipažinti ir išmokti duomenų apsaugos pareigūno įkeltą medžiagą į sistema, kuri padės jam išlaikyti testą. Po to kaip darbuotojas susipažįsta su pateikta medžiaga, jis gali laikyti testą. Testą galima laikyti neribotą skaičių kartų. Tiek bandymai laikyti testą, tiek ir pranešimas apie išlaikytą testą išsaugomi sistemoje.

Sistema sutikrina ar darbuotojas išlaikė testą ir išveda pranešimą ekrane, jog testas buvo išlaikytas/neišlaikytas, tuo pačiu metu sistema išsiunčia el. laišką duomenų apsaugos pareigūnui su vartotojo laikyto testo rezultatais, kad DAP galėtų sekti kaip sekasi jo įmonės darbuotojams laikyti testus.

Užklausos pateikimas DAP - čia suteikiama galimybė pranešti (tiek anonimiškai, tiek ir save identifikuojant) apie grupės įmonės pastebėtus pažeidimus ar rimtas problemines situacijas grupės vadovybės atstovams. Taip pat darbuotojas gali paklausti apie jam rūpimus klausimus susijusius su BDAR. El.paštu užklausa gaunantis duomenų apsaugos pareigūnas gali toliau tęsti el.pašto pagalba komunikacija su darbuotojais taip palaikydamas įmonės darbuotojų gerą žinių lygi ir kompetenciją.

A close up of a map

Description automatically generated

pav. 2 Vaizdusis paveikslėlis - Planuojama kurti sistema

### Verslo vykdomų užduočių analizė

* + - 1. Esminės užduotys

A picture containing bird

Description automatically generated

pav. 3 Esminės užduotys

## Verslo problemų, grėsmių ir neišnaudotų galimybių (SSGG) analizė

lentelė 3 SSGG matrica

|  |  |
| --- | --- |
| Stiprybės:   * Tiesioginis bendravimas; * Nereikalingi kompiuteriniai resursai. | Silpnybės:   * Brangūs žmogiškieji ištekliai; * Lėtas grįžtamasis ryšys; * Neautomatizuotas klausimyno tikrinimas; * Metodologijos nutekinimo rizika; * Netikslių duomenų pateikimas. |
| Grėsmės:   * Žmogiškųjų resursų trūkumas; * Neatliktas darbas per tam tikrą laiką; * Nekorektiškų duomenų gavimas. | Galimybės:   * Sistemos sukūrimas; * Automatizuotas rizikų ir grėsmių surašymas; * Duomenų koregavimas per trumpą laiką. |

## Verslo tobulinimo strategija

Kuriama PS sieks palengvinti ir pagerinti BDAR atitikties įvertinimo procesą įmonės viduje. Sistema leis grečiau ir patogiau užpildyti klausimyną taip sumažinant projekto laiko kaštus. Duomenų apsaugos pareigūnas arba sistemos administratorius gaus vieną klausimyna priskirtą įmonėje su jau pateiktais vartotojo rezultatais ir sugeneruotomis preliminariomis rizikomis bei rekomendacijomis, tai leis paspartinti viso proceso eigą.

Strategija:

1. Greitesnis klausimyno užpildymas:
   1. Pagreitinti klausimyno užpildymą 50%;
   2. Pagreitinti klausimyno tikrinimą ir rezultatų gavimą 200%;

1.3 Pagreitinti atitikties projekto eigą 30%.

1. Pagerinti įmonės BDAR atitiktį:

2.1 Duomenų apsaugos pareigūno darbo intensyvumo didinimas 25%;

2.2 Klaidų susijusių su BDAR pažeidimais mažinimas 200%.

## Užsakovo poreikių analizė

lentelė 4 Užsakovo poreikiai

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Operacinis tikslas | Resursai, reikalingi tikslui įgyvendinti | Prioritetas |
| 1.1 | Pagreitinti klausimyno užpildymą 50%; | Klausimyno pildymo, kūrimo sistema. Serveris sistemai paleisti. Duomenų bazė. | 1 |
| 1.2 | Pagreitinti klausimyno tikrinimą ir rezultatų gavimą 200% | Klausimyno pildymo, kūrimo sistema. Serveris sistemai paleisti. Duomenų bazė. Microsoft Office paketas. | 1 |
| 1.3 | Pagreitinti atitikties projekto eigą 30%. | Klausimyno pildymo, kūrimo sistema. Serveris sistemai paleisti. Duomenų bazė. Microsoft Office paketas. | 1 |
| 2.1 | Duomenų apsaugos pareigūno darbo intensyvumo didinimas 25%; | Klausimyno pildymo, kūrimo sistema. Serveris sistemai paleisti. Duomenų bazė | 2 |
| 2.2 | Klaidų susijusių su BDAR pažeidimais mažinimas 200%. | Klausimyno pildymo, kūrimo sistema. Serveris sistemai paleisti. Duomenų bazė. Microsoft Office paketas. | 1 |

## Sistemos naudojimo scenarijus

### Esamoji būklė

Dažniausiai įmonės nenaudojama jokios sistemos BDAR atitikčiai gerinti ir DAP darbo palengvinimui. Įmonėse BDAR atitikties klausimus sprendžia vienas žmogus,kuris susiduria su laiko resursų problema. Įvertinti BDAR atitiktį įmonėje yra sunkus ir sudėtingas darbas, kuri yra imlus laikui, tokiu atveju vsi pagrindiniai DAP darbai turėtų būti atliekami po atitikties įvertinimo proceso.

Įmonė privalo atlikti BDAR atitikties įsivertinimą, jog sumažintu galimas rizikas pažeisti reglamentą, tačiau dabartinėje situacijoje tai užtrunka per daug laiko ir pinigų todėl, jokios sistemos, kuri leistu tai įgyvendinti nėra sukurta. Klausimynai siunčiami kiekvienam darbuotojui/įmonei individualiai, kas yra labai neefektyvu ir užima daug laiko. Be to klausimynai darbuotojams dalinami ir popieriniame variante, jei įmonėje darbuotojų yra didelis kiekis – surinkti ir ištaisyti testus kainuoja labai daug laiko ir žmogiškųjų resursų, o tai įmonei kainuoja labai brangiai.

## Teikiamos naudos analizė

A close up of a map

Description automatically generated

pav. 7 Užduočių diagrama

Įmonės darbuotojas atliks vieną pagrindinę jam skirtą užduotį, dėl kurios ši sistema ir buvo kurta – užpildys klausimyną į sistemą. Klausimyno pildymas supaprastintas, kad pildymas užtrukų kuo mažesnį laiko tarpą, taip tausojant įmonės darbuotojo ir atitikties projekto laiką.

Duomenų apsaugos pareigūnas arba sistemos administratorius turi paruošti sistemą, jog darbuotojas galėtų laikyti testą. Tinkamam klausimyno pildymo parengimui reikalingos 3 užduotys: vartotojų administravimas, įmonių administravimas, klausimų administravimas. Visos šios užduotys yra tam, jog sistemoje galima būtų pridėti, ištrinti arba redaguoti vartotojus, įmones ir klausimus, kurie sudarys klausimyną. Esminė sistemos administartoriaus užduotis yra atsisiųsti jau sistemos sugeneruota galutinį klausimyną, kuriame bus pateiktos preliminarios rekomendacijos, rizikos ir rizikų svarba įmonei.

Sistemos administratoriaus pagrindinės užduotys yra palaikyti tinkamą sistemos veikimą ir ją prižiūrėti. Jis sukurs vartotojus sistemose, jiems priskirs reikiamas įmones, sukurs klausimyną. Pagrindinė šio aktoriaus veikla – sistemos palaikymas ir prižiūrėjimas.

## Išvados ir siūlymai

Sistema „GDPR Partners“ nėra sudėtinga sukurti, todėl ji nereikalauja didelio kiekio resursų – sistemos kūrėjai dirba nemokamai, nes jie atlieka praktika įmonėje, kainuoja tik darbų vadovas, kuris juos kuruoja. Taip pat PS kūrimas nėra imlus laikui, sistema galima sukurti su „Wix“ platforma, kuri yra lengvai išmokstama.

Nežiūrint į tai sistema puikiai tinka šiuometiniai rinkai, kadangi Bendrasis duomenų reglamentas skaičiuoja pirmus savo metus rinkoje ir yra aktuali tema kiekvienai Europos sąjungos šalies įmonei. Platforma lengva naudotis ir ji nekainuoja daug kaštų, todėl yra puiki prekė įmonėms.

„GDPR Partners“ ne tik palengvins įmonės DAP darbą, bet ir suteiks pridėtinės vertės įmonei, kadangi didins BDAR atitiktį taip mažindama rizikas pažeisti BDAR. Platforma kels darbuotojų kvalifikacija taip automatiškai gerindama įmonės bendrąjį paveikslą rinkoje.

# Reikalavimų specifikacija

## A close up of a logo Description automatically generatedFormuluojamos užduotys

### Pagrindinės užduotys

pav. 9 Užduočių diagrama

### Interfeiso darnos ir standartizavimo reikalavimai

lentelė 15 Interfeiso darnos ir standartizavimo reikalavimai

|  |  |
| --- | --- |
| Nr. | Reikalavimai |
| SR.1 | Vartotojui atvaizduojant „IT Klausimyno“ sistemos langus reikia laikytis „HTML“ meniu standarto. |
| SR.2 | Visi pranešimai apie klaidas, informaciniai pranešimai, perspėjimai turi būti suvienodinti, kad neblaškytų ir neklaidintų vartotojo |

### Pranešimų formulavimo reikalavimai

lentelė 16 Pranešimų formulavimo reikalavimai

|  |  |
| --- | --- |
| Nr. | Reikalavimai |
| PR.1 | Pranešimai turi būti pateikiami trumpi, aiškūs, vieno – dviejų sakinių. |
| PR.2 | Vartotojui turi būti pateikiami pasisveikinimo pranešimai. |
| PR.3 | Vartotojui turi būti pateikiami aiškūs klaidų pranešimai. |
| PR.4 | Pranešimai turi būti pateikiami naujame lange. |

## Funkciniai sistemos reikalavimai

### Dalykiniai reikalavimai

**Reikalavimo statusas:**

* E – esminis (privalomas) reikalavimas;
* D – pageidavimas;
* O– papildomas reikalavimas.

**Reikalavimų galiojimo laikas:**

* S – pastovus reikalavimas;
* U – sąlyginai pastovus reikalavimas;
* T – laikinas reikalavimas.

**Kritiškumo laipsnis:**

* S – sunkios pasekmės;
* A – apysunkės pasekmės;
* L – lengvos pasekmės.

lentelė 18 Dalykiniai reikalavimai

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RNr. | Statusas (E, D, O) | Galiojimo laikas  (S, U, T) | Kritiškumo laipsnis  (S, A, L) | Užduoties Nr. | Reikalavimai |
| DR.1 | E | U | S | UZ.1 | Sistema turi leisti vartotojui prisijungti prie savo paskyros |
| DR.2 | E | S | S | UZ.2 | Sistema turi leisti administratoriui prisijungti prie savo paskyros |
| DR.3 | E | U | S | UZ.3 | Sistema turi leisti vartotojui užpildyti klausimyną. |
| DR.4 | E | U | S | UZ.4 | Sistema turi leisti vartotojui pateikti klausimyną galutinei peržiūrai. |
| DR.5 | E | S | A | UZ.5 | Sistemos administratorius turi turėti galimybę sukurti įmonę. |
| DR.6 | E | S | A | UZ.6 | Sistemos administratorius turi turėti galimybę redaguoti įmonės pavadinimą. |
| DR.7 | E | S | L | UZ.7 | Sistemos administratorius turi turėti galimybę ištrinti įmonę. |
| DR.8 | E | S | S | UZ.8 | Sistemos administratorius turi turėti galimybę sukurti vartotoją. |
| DR.9 | E | S | A | UZ.9 | Sistemos administratorius turi turėti galimybę redaguoti vartotojo duomenis. |
| DR.10 | E | S | L | UZ.10 | Sistemos administratorius turi turėti galimybę ištrinti vartotoją. |
| DR.11 | D | U | A | UZ.11 | Sistemos administratorius turi turėti galimybę aktyvuoti/deaktyvuoti vartotojo galimybę prisijungti prie sistemos. |
| DR.12 | E | S | A | UZ.12 | Sistemos administratorius turi turėti galimybę sukurti naują klausimą. |
| DR.13 | E | S | A | UZ.13 | Sistemos administratorius turi turėti galimybę sukurti redaguoti klausimo duomenis. |
| DR.14 | E | S | A | UZ.14 | Sistemos administratorius turi turėti galimybę ištrinti klausimą. |
| DR.15 | E | S | S | UZ.15 | Sistemos administratorius turi turėti galimybę automatiškai sugeneruoti klausimyno rizikas ir rekomendacijas su jų svarba. |
| DR.16 | E | S | S | UZ.16 | Sistemos administratorius turi turėti galimybę atsisiųsti klausimyną. |

### Pagalbinės sistemos funkcijos

lentelė 19 Pagalbinės sistemos funkcijos reikalavimai

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RNr. | Statusas (E, D, O) | Galiojimo laikas  (S, U, T) | Kritiškumo laipsnis  (S, A, L) | Užduoties Nr. | Reikalavimai |
| PF.1 | E | S | A | UZ.1 | Vartotojas turi matyti administratoriaus kontaktus susisiekimui |
| PF.2 | E | U | S | UZ.2 | Vartotojas turi gauti paaiškinimą klausimyno pildymui |
| PF.3 | E | S | S | UZ.3 | Sistemos administratoriui turi būti pateikiamos instrukcijos apie sistemos valdymą bei prižiūrėjimą. |

## Nefunkciniai reikalavimai

## Vidinio interfeiso reikalavimai

## Operacinės sistemos naudojimo reikalavimai

lentelė 20 Operacinės sistemos naudojimo reikalavimai

|  |  |
| --- | --- |
| Nr. | Reikalavimas |
| OSR.1 | Sistema turi būti pritaikyta Windows operacinei sistemai |

## Sąveikos su duomenų bazėmis reikalavimai

lentelė 21 Sąveikos su duomenų bazėmis reikalavimai

|  |  |
| --- | --- |
| Nr. | Reikalavimas |
| SDBR.1 | Visi duomenys esantys sistemoje turi būti saugomi reliacinėje duomenų bazėje |
| SDBR.2 | Visi duomenų pakeitimai turi būti automatiškai išsaugoti reliacinėje duomenų bazėje |

## Dokumentų mainų reikalavimai

lentelė 22 Dokumentų mainų reikalavimai

|  |  |
| --- | --- |
| Nr. | Reikalavimas |
| DMR.1 | Sistema turi sugeneruoti klausimyną .xlsx formatu |
| DMR.2 | Sistema turi leisti atsisiųsti klausimyną .xlsx formatu |

## Programavimo aplinkos reikalavimai

lentelė 24 Programavimo aplinkos reikalavimai

|  |  |
| --- | --- |
| Nr. | Reikalavimas |
| PAR.1 | Sistema turi būti programuojama „Angular“ frontend karkaso pagrindu. |
| PAR.2 | Sistema turi būti programuojama „TypeScript ”, „JavaScript“, „HTML“, „CSS“ programavimo kalbomis |

## Veikimo reikalavimai

## Tikslumo reikalavimai

## Vaizdavimo tikslumo reikalavimai

lentelė 25 Vaizdavimo tikslumo reikalavimai

|  |  |
| --- | --- |
| Nr. | Reikalavimas |
| VTR.1 | Vartotojo sąsajoje turi būti naudojamos ne daugiau kaip trys spalvos viename lange |
| VTR.2 | Visi valdymo(trynimas, redagavimas, pridėjimas) mygtukai turi rikiuotis lango dešinėje pusėje |
| VTR.3 | Pagrindiniai meniu mygtukai turi būti išsidėstę lango viršuje kaip antraštės juosta |

## Patikimumo reikalavimai

lentelė 27 Patikimumo reikalavimai

|  |  |
| --- | --- |
| Nr. | Reikalavimas |
| PR.1 | Sistemos klaidos, trykiai turi būti sutvarkomi ne ilgiau negu per valandą |

## Robastiškumo reikalavimai

lentelė 28 Robastiškumo reikalavimai

|  |  |
| --- | --- |
| Nr. | Reikalavimai |
| RR.1 | Sistema turi turėti duomenų kopijas, kad sistemos trykio metu prarasti duomenys būtų ne senesni nei viena diena. |

## Našumo reikalavimai

lentelė 29 Našumo reikalavimai

|  |  |
| --- | --- |
| Nr. | Reikalavimai |
| NR.1 | Vartotojo užklausos turi būti įvykdytos ne ilgiau kaip per keturias sekundes. |
| NR.2 | Turi būti palaikoma ne mažiau kaip 200 užklausų per sekundę neviršijus 0,15% srauto klaidų skaičiaus. |

## Diegimo reikalavimai

## Ruošinio reikalavimai

lentelė 30 Ruošinio reikalavimai

|  |  |
| --- | --- |
| Nr. | Reikalavimai |
| RUR.1 | Sistemos ruošinys turi neviršyti 2GB dydžio. |
| RUR.2 | Sistemos ruošinys turi būti patalpintas į internetą, kuriame veiktu „debesų technologijomis“ paremtuose serveriuose, kad vartotojas galėtų iškarto naudotis sistema tik pasirašius sutartį |

## Instaliavimo reikalavimai

Nėra, kadangi sistema veikia kaip PaaS (angl. platforma as a service) paslauga per Internetinę naršyklę.

## Pradinio duomenų bazių kaupimo reikalavimai

lentelė 31 Pradinio duomenų bazių kaupimo reikalavimai

|  |  |
| --- | --- |
| Nr. | Reikalavimai |
| PDBKR.1 | Pradinius duomenis turi suvesti sistemos administratorius. |
| PDBKR.2 | Pradiniai duomenys turi būti paruošti .csv formato faile. |

## Apsaugos reikalavimai

lentelė 34 Apsaugos reikalavimai

|  |  |
| --- | --- |
| Nr. | Reikalavimai |
| AR.1 | Sistemos paskyros privalo būti apsaugotos slaptažodžiu |

## Juridiniai reikalavimai

lentelė 35 Juridiniai reikalavimai

|  |  |
| --- | --- |
| Nr. | Reikalavimai |
| JR.1 | Sistema turi nepažeist Lietuvos Respublikos mokėjimų įstatymo 1999 m. spalio 28 d. Nr. VIII-1370. |
| JR.2 | Sistema turi atitikti Bendrojo duomenų apsaugos reglamento rekomendacijas. |

# Programų sistemos projektavimas

## Programų sistemos projektiniai reikalavimai

### Programų sistemos dekompozicija

A close up of a map

Description automatically generated

pav. 13 UML komponentų diagrama

Vartotojo sąsajos komponentas turi savyje užklausos modeli, vartotojai šiame komponente gali pateikti užklausa DAP arba peržiūrėti atsakymus į pateiktas užklausas. Šis komponentas turi sąsaja su administratoriaus aplinkos moduliu, kadangi administratorius gali daryti keitimus kiekviename modulyje. Taip pat Vartotojo modulis turi sąsaja su duomenų baze kadangi reikia viską išsaugoti.

Administratoriaus aplinkos modulis savyje turi Vartotojų komponentą, kadangi jis gali valdyti visus darbuotojų paskyras, jas ištrinti arba sukurti naujas. Tuo pačiu principu jis turi ir sąsaja su Vartotojų moduliu. Taip pat Administratorius turi išsaugoti visus vartotojų duomenis, todėl jis turi sąsaja ir su duomenų saugyklos moduliu.

Duomenų saugykla turi sąsaja su visais moduliais, kadangi visi moduliai ir jų komponentai gali įdėti ir pasiimti medžiaga iš duomenų bazės modulio. Taip pat savyje jis turi testų ir užklausų komponentus, nes juos išsaugoja duomenų bazėje.

### Reikalavimų lokalizavimo matrica

Šiame poskyryje pateikiama reikalavimų lokalizavimo matrica

*3.1 lentelė. Reikalavimų lokalizavimo matrica*

|  |  |  |  |
| --- | --- | --- | --- |
| Reikalavimai | Vartotojo sąsajos modulis | Administratoriaus aplinkos modulis | Duomenų saugyklos modulis |
| SR.1 | Prisijungimo komponente, Klausimyno pildymas komponente | Klausimyno administravimas komponente, Vartotojų administravimas komponente, Imonių administravimas komponente, Prisijungimas komponente | - |
| SR.2 | Prisijungimo komponente, Klausimyno pildymas komponente | Klausimyno administravimas komponente, Vartotojų administravimas komponente, Imonių administravimas komponente, Prisijungimas komponente | - |
| PR.1 | Klausimyno pildymas komponente | Klausimyno administravimas komponente, Vartotojų administravimas komponente, Imonių administravimas komponente | X |
| PR.2 | Prisijungimo komponente, Klausimyno pildymas komponente | Klausimyno administravimas komponente, Vartotojų administravimas komponente, Imonių administravimas komponente, Prisijungimas komponente | - |
| PR.3 | Prisijungimo komponente, Klausimyno pildymas komponente | Klausimyno administravimas komponente, Vartotojų administravimas komponente, Imonių administravimas komponente, Prisijungimas komponente | - |
| PR.4 | Prisijungimo komponente, Klausimyno pildymas komponente | Klausimyno administravimas komponente, Vartotojų administravimas komponente, Imonių administravimas komponente, Prisijungimas komponente | - |
| DR.1 | X | X | X |
| DR.2 | X | X | X |
| DR.3 | X | - | - |
| DR.4 | X | - | - |
| DR.5 | - | X | X |
| DR.6 | - | X | X |
| DR.7 | - | X | X |
| DR.8 | - | X | X |
| DR.9 | - | X | X |
| DR.10 | - | X | X |
| DR.11 | - | X | X |
| DR.12 | - | X | X |
| DR.13 | - | X | X |
| DR.14 | - | X | X |
| DR.15 | - | X | X |
| DR.16 | X | - | - |
| PF.1 | X | - | - |
| PF.2 | X | X | X |
| PF.3 | X | X | X |
| OSR.1 | X | - | X |
| SDBR.1 | X | - | - |
| SDBR.2 | X | - | X |
| DMR.1 | X | - | - |
| DMR.2 | - | X | - |
| PAR.1 | X | - | - |
| PAR.2 |  |  |  |
| VTR.1 | X | X | - |
| VTR.2 | - | X | X |
| VTR.3 | X | X | X |
| PR.1 | X | X | X |
| RR.1 | - | - | X |
| NR.1 | X | - | - |
| NR.2 | X | - | X |
| RUR.1 | X | X | X |
| RUR.2 | X | X | X |
| PDBKR.1 | X | X | X |
| PDBKR.2 | X | X | X |
| AR.1 | X | - | - |
| JR.1 | X | X | X |
| JR.2 | X | X | X |

## Programų sistemos architektūra

### A close up of text on a white background Description automatically generatedUžduotys ir jų vykdymo scenarijai

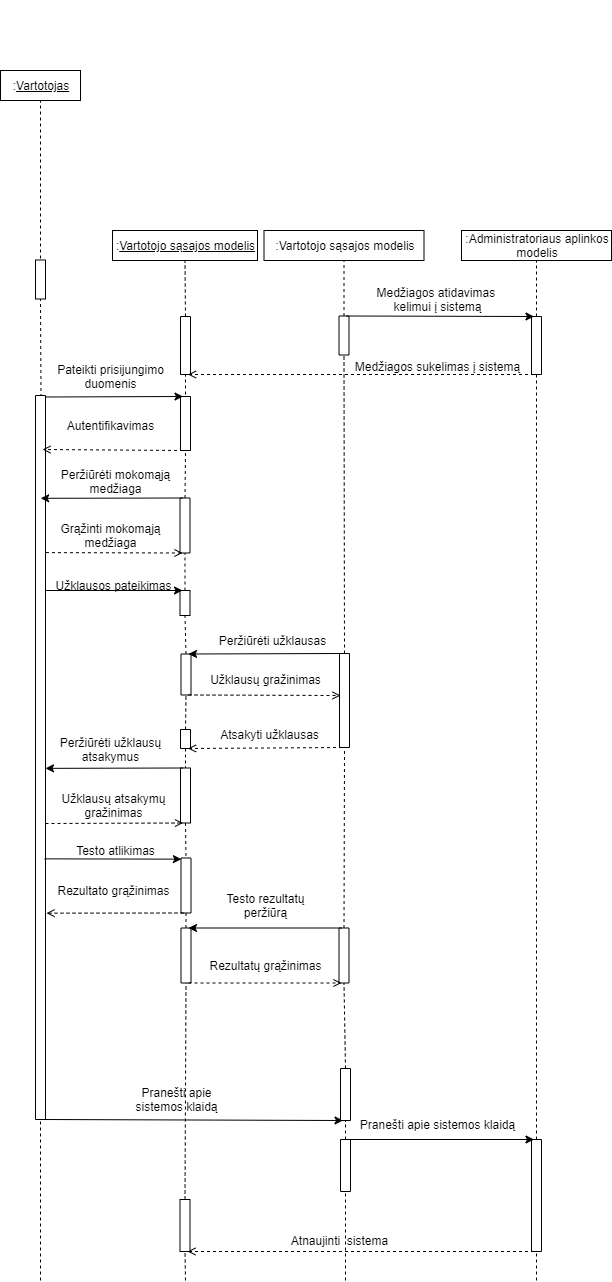
pav. 14 Informacinės sistemos užduočių diagrama

A screenshot of a social media post

Description automatically generated

lentelė 36 Testo atlikimas

|  |  |
| --- | --- |
| Užduotis | Testo atlikimas |
| Moduliai | Sistema, Duomenų apsaugos pareigūnas, Sistemos administratorius |
| Seka | Užd 1. Vartotojas atlieka testas  Užd 6. Sistema gražina testo rezultatus  Užd 5. Administratorius peržiūri testo rezultatus  Užd 6. Sistema gražina testo rezultatus |



pav. 16 Sekų diagrama Medžiagos kėlimas į sistemą UML

lentelė 37 Medžiagos kėlimas į sistemą

|  |  |
| --- | --- |
| Užduotis | Medžiagos kėlimas į sistemą |
| Moduliai | Sistema, Duomenų apsaugos pareigūnas, Sistemos administratorius |
| Seka | Užd 4. Vartotojas atiduoda administratoriui įkelti medžiaga  Užd 4. Administratorius įkelia medžiagą į sistemą |

A close up of a map

Description automatically generated

pav. 17 Sekų diagrama „Sistemos atnaujinimas“ UML

lentelė 38 Sistemos atnaujinimas

|  |  |
| --- | --- |
| Užduotis | Sistemos atnaujinimas |
| Moduliai | Sistema, Duomenų apsaugos pareigūnas, Sistemos administratorius |
| Seka | Užd 3. Vartotojas praneša apie klaidą sistemoje  Užd 6. Administratorius klaidą ištaiso |

A screenshot of a social media post

Description automatically generated

pav. 18 Sekų diagrama „Vartotojų sukūrimas“ UML

lentelė 39 Vartotojų sukūrimas

|  |  |
| --- | --- |
| Užduotis | Vartotojų sukūrimas |
| Moduliai | Sistema, Duomenų apsaugos pareigūnas, Sistemos administratorius |
| Seka | Užd 7. Administratorius sukuria vartotojus  Užd 3. Sistema duoda prisijungimus vartotojams |

### A screenshot of a cell phone Description automatically generated

pav. 19 Sekų diagrama Užklausos pateikimas UML

lentelė 40 Užklausos pateikimas

|  |  |
| --- | --- |
| Užduotis | Užklausos pateikimas |
| Moduliai | Sistema, Duomenų apsaugos pareigūnas, Sistemos administratorius |
| Seka | Užd 3. Vartotojas pateikia užklausa  Užd 3. Administratorius peržiūri užklausas  Užd 6. Sistema gražina užklausas  Užd 3. Administratorius atsako užklausą  Užd 6. Vartotojas peržiūri užklausą  Užd 3. Sistema gražina užklausą |

### PS struktūros modelis

### Klasių ir objektų diagramos

A close up of a map

Description automatically generated

pav. 20 Klasių ir objektų UML

Kiekviena paskyra turi unikalų ID. Paskyrai priklauso gali atlikti daug užklausų ir daug testo laikymų. Paskyra taip pat turi prisijungimo duomenis – vartotojo vardą ir slaptažodį, paskyroje taip pat yra el. paštas dėl autentifikavimosi.

Kiekviena užklausa gali turėti daug vartotojų. Kiekviena užklausa turi unikalų ID, datą kada ji buvo sukurta ir patį užklausos tekstą.

Testo laikymas turi vartotojus, kurie gali daug kartų testą laikyti, taip pat testo laikymas turi daug testų, kuruos jis paduos vartotojams. Testo laikymas turi unikalų ID, išlaikymo rezultatą (Score) ir vartotojo el. paštą, kad autentifikuotų laikiusį vartotoją.

Testas turi testo laikymas, viena testą galima laikyti daug kartų. Testas turi unikalų ID, patį tekstą ir sukūrimo datą.

Paskyra su ID=1 priklauso vartotojui, kurio el.paštas yra [darbuotojas@gmail.com](mailto:darbuotojas@gmail.com). Vartotojo prisijungimas prie sistemos yra vartotojo vardas – vartotojas1 ir slaptažodis – slaptažodis1.

Užklausa su ID=1 yra sukurtas 2019-12-08 ir joje parašyta – Užklausos tekstas.

Testo laikymas turi ID=1, testą laikė darbuotojas – [darbuotojas@gmail.com](mailto:darbuotojas@gmail.com), o jo laikymo rezultatas yra 83,3.

Testas turi unikalų ID=1, jis sukurtas yra 2019-12-08 ir jame yra tekstas – Testo tekstas.

A screenshot of a cell phone

Description automatically generated

pav. 21 Klasių ir objektų 2 UML

### A close up of a map Description automatically generatedEsybių gyvavimo ciklo modelis

[užklausti]

[atlikti]

[atlikti]

[peržiūrėti]

pav. 22 UML būsenų diagrama

Sistemoje galima skaityti mokomąją medžiagą bei parašyti užklausą, šie veiksmai vienas nuo kito nepriklauso ir neprašo, jog atlikti vieną reikią būtinai įgyvendinti kitą. Taip pat sistemoje galima atlikti testą, kad atlikti testą reikėtų peržiūrėti pateiktą medžiagą. Atlikus testą galimą peržiūrėti testo rezultatus ir užbaigti sistemos darbą. Sistemos darbą galima užbaigti bet kada, nepriklausomai nuo įvykdytų užduočių.

## A screenshot of a cell phone Description automatically generatedProgramų sistemos maketai

pav. 23 Programų sistemų maketų UML

Sistemos komponentai yra suskirstyti į Internetinės svetainės serverį ir duomenų saugyklą. Klientas per savo kompiuterį gali pasiekti aplikaciją, kurioje vyksta užklausų siuntimas, testo atlikimas ir mokomosios medžiagos skaitymas. Aplikacijos serveris saugo duomenis apie paskyras, testus ir mokomąją medžiagą.

# Testavimas

## Testavimo scenarijai

## Testavimo atvejis 1

Testuojamas vartotojo vardo priminimo scenarijus.

Testuojamo reikalavimo RS numeris - PF.2

|  |
| --- |
| **Testavimo atvejo ID: a**1 |
| **Testavimo prioritetas:** Aukštas |
| **Modulio pavadinimas:** Prisijungimo ekranas |
| **Testo atvejo pavadinimas:** Sėkmingasvartotojo vardo priminimas |
| **Aprašymas:** Ištestuoti ar programinė įranga sėkmingai primena vartotojui apie jo vartotojo vardą internetinėje svetainėje |
| **Išankstinės sąlygos:** Naudotojasturi turėti paskyrąduomenų bazėje su el. Pašto adresu ([pvz@mail.com](mailto:pvz@mail.com)), turėti prieigą prie nurodyto el. Pašto |
| **Sistemos būsena po testavimo:** Serverio žurnale užfiksuotas vartotojo vardo išsiuntimas ir sėkmingas prisijungimas |

lentelė 41 Testavimas reikalavimo - PF.2

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Žingsnis** | **Testo žingsnis** | **Testo duomenis** | **Laukiamas rezultatas** | **Gautas rezultatas** | **Statusas** | **Pastabos** |
| 1. | Atsidaryti interneto naršyklę |  | Atidaroma naršyklė |  |  | Naršyklei apribojimų nėra |
| 2. | URL lange įvedame programos adresą | URL programos | Atidaroma programa |  |  |  |
| 3. | Spausti mygtuką „Priminti“ |  | Programa paprašo įvesti el. Paštą |  |  |  |
| 4. | Suvedame el. Pašto adresą | Teisingas El. Pašto adresas |  |  |  |  |
| 5. | Spaudžiamas mygtukas priminti |  | Ekrane parodomas pranešimas ar laiškas su naudotojo vartotojo vardu išsiunčiamas į jo el. paštą |  |  |  |
| 6. | Atidaryti el. Paštą |  | Gautas el. Laiškas kuriame pateiktas naudotojo vartotojo vardas |  |  |  |
| 7. | Įvesti gautą vartotojo vardą ir slaptažodį | Slaptažodis ir el. Pašte gautas vartotojo vardas |  |  |  |  |
| 8. | Paspausti mygtuką „Prisijungti“ |  | Ekrane pateikiama žinutė „SVEIKI“ | Ekrane pateikiama žinutė „SVEIKI“ | Testas pavyko |  |

## Testavimo atvejis 2

Testuojamo reikalavimo RS numeris - PF.2

|  |
| --- |
| **Testavimo atvejo ID: a**2 |
| **Testavimo prioritetas:** Aukštas |
| **Modulio pavadinimas:** Prisijungimo ekranas |
| **Testo atvejo pavadinimas:** Nesėkmingasvartotojo vardo priminimas |
| **Aprašymas:** Ištestuoti ar programinė įranga sėkmingai praneša, kad vartotojas neegzistuoja |
| **Išankstinės sąlygos:** Naudotojas pamiršo prisijungimo duomenis; |
| **Sistemos būsena po testavimo:** Serverio žurnale užfiksuotas nesėkmingas vartotojo vardo priminimas. |

lentelė 42 Testavimas reikalavimo - PF.1

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Žingsnis** | **Testo žingsnis** | **Testo duomenis** | **Laukiamas rezultatas** | **Gautas rezultatas** | **Statusas** | **Pastabos** |
| 1. | Atsidaryti interneto naršyklę |  | Atidaroma naršyklė |  |  | Naršyklei apribojimų nėra |
| 2. | URL lange įvedame programos adresą | URL programos | Atidaroma programa |  |  |  |
| 3. | Spausti mygtuką „Priminti“ |  | Programa paprašo įvesti el. Paštą |  |  |  |
| 4. | Suvedame el. Pašto adresą | Neteisingas El. Pašto adresas |  |  |  |  |
| 5. | Spaudžiamas mygtukas priminti |  | Ekrane parodomas pranešimas, kad nėra vartotojo su pateiktu el. Pašto adresu | Ekrane parodomas pranešimas, kad nėra vartotojo su pateiktu el. Pašto adresu | Testas pavyko |  |

## Testavimo atvejis 3

Testuojamo reikalavimo RS numeris - PF.2

|  |
| --- |
| **Testavimo atvejo ID: a3** |
| **Testavimo prioritetas:** Aukštas |
| **Modulio pavadinimas:** Prisijungimo ekranas |
| **Testo atvejo pavadinimas:** Neteisingai įvestas el. Pašto adresas vartotojo vardo priminimo lange |
| **Aprašymas:** Ištestuoti ar programinė įranga sėkmingai praneša, kad vartotojas neteisingai įvėdė el. Pašto adresą |
| **Išankstinės sąlygos:** Naudotojas turisugalvoti neteisingą el. Paštą (pvz. Be @ ženklo, be nuorodos į el. Pašto svetaine (gmail.com, yahoo.com)) |
| **Sistemos būsena po testavimo:** serverio žurnale užfiksuotas nesėkmingas vartotojo vardo priminimas |

lentelė 43 Testavimas reikalavimo - PF.2

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Žingsnis** | **Testo žingsnis** | **Testo duomenis** | **Laukiamas rezultatas** | **Gautas rezultatas** | **Statusas** | **Pastabos** |
| 1 | Atsidaryti interneto naršyklę |  | Atidaroma naršyklė |  |  | Naršyklei apribojimų nėra |
| 2 | URL lange įvedame programos adresą | URL programos | Atidaroma programa |  |  |  |
| 3 | Spausti mygtuką „Priminti“ |  | Programa paprašo įvesti el. Paštą |  |  |  |
| 4 | Suvedame el. Pašto adresą | Neteisingas El. Pašto adresas |  |  |  |  |
| 5 | Spaudžiamas mygtukas priminti |  | Ekrane parodomas „El. paštas įvestas neteisingai“ | Ekrane parodomas pranešimas, kad įvestas el. Paštas yra parašytas su klaidomis | Testas pavyko |  |

## Testavimo atvejai

## Statinis testavimo atvejis

lentelė 44 Statinis testavimo atvejis

|  |  |  |  |
| --- | --- | --- | --- |
| **Nr.** | **KS reikalavimas/klausimas** | **Ar tenkinamas (taip, ne, iš dalies)** | **Pastabos, prielaidos** |
| 1. | Ar yra reikalavimai užpildyti? | Iš dalies | Naudotojo vardo ir slaptažodžio validacijai netiksliai nurodyti reikalavimai |
| 2. | Ar visi reikalavimai yra vienareikšmiškai atpažįstami? | Ne | Nesunumeruota, nesužymėta |
| 3. | Ar reikalavimai yra aiškūs ir tinkamai suskirstyti į prioritetus? | Ne | Nepateikta kokia užduočių svarba |
| 4. | Ar reikalavimai yra nuoseklūs? (t. y. nėra vidinių prieštaravimų) | Ne | 5 ir 6 kontradikcija, vienas sako kad galima bandyti prisijungti 5 kartus, kitas sako kad galima prisijungti bandyti neribotą skaičių kartų |
| 5. | Ar reikalavimų rinkinys tinkamai sprendžia visas tinkamas išimties sąlygas? | Taip | Visi reikalavimai sprendžiami teisingai |
| 6. | Ar reikalavimų rinkinys tinkamai sprendžia ribines sąlygas? | Iš dalies | Pateikta tik pavyzdys slaptažodžio ribojimams, tačiau nenurodyta tiksliai |
| 7. | Ar reikalavimai yra įgyvendinami? (t. y. yra reikalavimų rinkinio sprendimas) | Taip |  |
| 8. | Ar reikalavimus galima įgyvendinti atsižvelgiant į žinomus suvaržymus? | Taip |  |
| 9. | Ar pakanka reikalavimų? (ty, jie gali būti siunčiami į gerbiamų plėtros organizacija ir turi pagrįstą tikimybę gaminti produktą, kaip buvo pageidaujama) | Ne | Ankščiau pateiktos pastabos |
| 10. | Ar šie paprasčiausi nustatyti reikalavimai, atitinka suinteresuotųjų šalių poreikius? | Taip |  |
| 11. | Ar visos kryžminės nuorodos į kitus reikalavimus yra teisingos? | Ne | Nėra |
| 12. | Ar buvo apsvarstyti funkciniai ir nefunkciniai reikalavimai? | Taip |  |
| 13. | Ar reikalavimai nėra dubliuojami ir neatitinka kitų reikalavimų? | Ne |  |
| 14. | Ar kiekvienas reikalavimas parašytas nuoseklia, aiškia, glausta kalba? | Iš dalies | Naudojama netinkama kalba kai kuriose vietose, kursorius – žymeklis |
| 15. | Ar kiekvienas reikalavimas turi tik vieną aiškinimą? Jei terminas gali turėti keletą reikšmių, ar jis apibrėžtas? | Ne |  |
| 16. | Ar kiekvienas reikalavimas yra patikrinamas atliekant testavimą, demonstravimą, peržiūrą ar analizę? | Taip |  |
| 17. | Ar yra išmatuojamų priimtinumo kriterijų dėl kiekvieno funkcinio ir nefunkcinio reikalavimo? | Ne | Operacijų veikimo trukmės nepateiktos  Nepateikiama kai išsiunčiamas el. laiškas naudotojui |

## 

## Automatinis testavimo atvejis

Testavimas buvo vykdomas su „Katalon“ programa.

Testuojama buvo prisijungimas prie sistemos bei užklausos išsiuntimas Duomenų apsaugos pareigūnui.

**Testo kodas su Java (Webdriver + Junit):**

package com.example.tests;

import java.util.regex.Pattern;

import java.util.concurrent.TimeUnit;

import org.junit.\*;

import static org.junit.Assert.\*;

import static org.hamcrest.CoreMatchers.\*;

import org.openqa.selenium.\*;

import org.openqa.selenium.firefox.FirefoxDriver;

import org.openqa.selenium.support.ui.Select;

public class TESTPOSITIVE {

private WebDriver driver;

private String baseUrl;

private boolean acceptNextAlert = true;

private StringBuffer verificationErrors = new StringBuffer();

@Before

public void setUp() throws Exception {

driver = new FirefoxDriver();

baseUrl = "https://www.katalon.com/";

driver.manage().timeouts().implicitlyWait(30, TimeUnit.SECONDS);

}

@Test

public void testPOSITIVE() throws Exception {

driver.get("https://www.privacypartners.lt/cd");

driver.findElement(By.id("enterPasswordDialogpasswordInputinput")).clear();

driver.findElement(By.id("enterPasswordDialogpasswordInputinput")).sendKeys("SLAPTAŽODIS");

driver.findElement(By.id("enterPasswordDialogokButton")).click();

driver.findElement(By.id("comp-jsbn3y1wlabel")).click();

driver.findElement(By.id("enterPasswordDialogpasswordInputinput")).clear();

driver.findElement(By.id("enterPasswordDialogpasswordInputinput")).sendKeys("Privacy");

driver.findElement(By.id("enterPasswordDialogpasswordInputinput")).click();

driver.findElement(By.id("enterPasswordDialogpasswordInputinput")).clear();

driver.findElement(By.id("enterPasswordDialogpasswordInputinput")).sendKeys("SLAPTAŽODIS");

");

driver.findElement(By.id("enterPasswordDialogpasswordInputinput")).sendKeys(Keys.ENTER);

driver.findElement(By.id("comp-jsbnaj68radio0text")).click();

driver.findElement(By.id("comp-jsbnaj73radio1circle")).click();

driver.findElement(By.id("field1")).click();

driver.findElement(By.id("field1")).clear();

driver.findElement(By.id("field1")).sendKeys("TESTAS");

driver.findElement(By.id("field2")).click();

driver.findElement(By.id("field2")).clear();

driver.findElement(By.id("field2")).sendKeys("TESTAS");

driver.findElement(By.id("field3")).click();

driver.findElement(By.id("field3")).clear();

driver.findElement(By.id("field3")).sendKeys("mantas.sebeika@privacypartners.lt");

driver.findElement(By.id("comp-jsbnaj8sfieldMessage")).click();

driver.findElement(By.id("comp-jsbnaj8sfieldMessage")).clear();

driver.findElement(By.id("comp-jsbnaj8sfieldMessage")).sendKeys("TESTO");

driver.findElement(By.id("comp-jsbnaj8ssubmit")).click();

// ERROR: Caught exception [ERROR: Unsupported command [captureEntirePageScreenshot | SS | SS]]

}

@After

public void tearDown() throws Exception {

driver.quit();

String verificationErrorString = verificationErrors.toString();

if (!"".equals(verificationErrorString)) {

fail(verificationErrorString);

}

}

private boolean isElementPresent(By by) {

try {

driver.findElement(by);

return true;

} catch (NoSuchElementException e) {

return false;

}

}

private boolean isAlertPresent() {

try {

driver.switchTo().alert();

return true;

} catch (NoAlertPresentException e) {

return false;

}

}

private String closeAlertAndGetItsText() {

try {

Alert = driver.switchTo().alert();

String alertText = alert.getText();

if (acceptNextAlert) {

alert.accept();

} else {

alert.dismiss();

}

return alertText;

} finally {

acceptNextAlert = true;

}

}

}

## Naudotojų istorijos

## Naudotojo istorija 1

* **Kaip** prisiregistravęs naudotojas ir prisijungiant prie tinklapio ne pirmą kartą;
* **Aš noriu** galėti prisijungti prie tinklapio;
* **Tam kad** turėčiau prieigą prie tinklapio dedikuoto darbuotojams;
* **Scenarijus**: Sistemoje egzistuojantis naudotojas prisijungia su teisingais duomenimis;
* Jau nustačius, kad naudotojas yra prisiregistravęs įmonės darbuotojas;
* Ir jis yra prisijungimo lange;
* Kai įveda teisingus prisijungimo duomenis - Vartotojo vardą ir slaptažodį;
* Parodomas vartotojams dedikuotas puslapis;
* Sistema prijungia prie tinklapio dedikuoto įmonės darbuotojams.

## Naudotojo istorija 2

* **Kaip** prisiregistravęs naudotojas;
* **Aš noriu** būti informuotasapie neteisingai įvestus prisijungimo duomenis;
* **Tam kad** galėčiau juos pataisyti ir bandyti prisijungti dar kartą;
* **Scenarijus**: Sistemoje egzistuojantis naudotojas bando prisijungti su neteisingais duomenis prie sistemos;
* Jau nustačius kad naudotojas yra prisiregistravęs prie sistemos;
* Ir vartotojas prisijungimo lange;
* Kai jis įveda neteisingus prisijungimo duomenis;
* Paspaudžia mygtuką prisijungti;
* Tada sistema praneša naudotojui apie neteisingai įvestus duomenis ir žymeklį pastato „Vartotojo vardo“ lauko.

# Išvados

Išanalizavus kuriamos „GDPR Partners“ internetinės sistemos poreikių specifikaciją buvo išsiaiškinti kuriamos sistemos verslo poreikiai, nustatytos sistemos silpnosios vietos, kritinės klaidos bei grėsmės. Taip pat analizės metu buvo įvertinti ekonominiai kaštai. Atlikus reikalavimų specifikaciją buvo išsiaiškintos ir nustatytos sistemos ribos, jos veikimas, prieigos ir atliekami veiksmai. Sistemos projektavime metu buvo sukurtas abstraktus sistemos prototipas bei apibrėžti komponentai, jų klasės ir sąveika tarpusavyje. Veikiančiai sistemai buvo atliktas funkcionalumų testavimas, nustatytas atitikimas reikalavimams ir verslo poreikiams. Sistema buvo realizuota pagal jai iškeltus reikalavimus ir suprojektuotą architektūrą. Analizės metu pastebėta, jog laikantis visų nurodytų punktų sistema dažnai keisdavosi ir būdavo taisomos prieš tai padarytos klaidos, todėl sistemos kūrimo procesas yra privalomas norint įgyvendinti veikiančia sistema, kuri neturi daug trikdžių, klaidų ir būtų paklausi rinkoje.

„GDPR Partners“ sistema leis įmonėms pakelti darbuotojų kompetenciją bei padidinti Bendrojo duomenų apsaugos atitiktį įmonėje. Sistemos pagalbą apmokius žmones bei padidinti jų kompetenciją automatiškai padidėja ir įmonės vertė bei sumažėja rizikingumas pažeisti įstatymus ir reglamentus susijusius su duomenų apsaugą. Taip pat išvengiama didelių nuotolių, kadangi už duomenų apsaugos pažeidimus įmonė gali būti baudžiama iki 4 proc. metinės apyvartos, o tai gali būti labai didelis smūgis kai kurioms įmonėms.

Taip pat, naudojantis sistema bus padidintas duomenų apsaugos pareigūno darbo našumas, kadangi, DAP nereikės atlikinėti papildomų darbų, kuriuos sistemos pagalbą jis įgyvendins kur kas greičiau bei efektyviau. Taip duomenų apsaugos pareigūnas sistemos pagalbą sumažins rizikas ne tik iš darbuotojų pusės bet taip pat galės vykdyti savo tiesioginį darbą ir padėti įmonei tvarkytis su duomenų apsaugą.

Taigi, atsižvelgus į visus sistemai keliamus reikalavimus jos kūrimo metu bei laikantis teisingų kūrimo principų galima ne tik sukurti puikiai veikiančia ir efektyvia sistema, bet ir jos pagalbą padidinti įmonės darbo našumą bei sumažinti rizikas joje.

# Tyrimo projektinė dalis

# Infrastruktūros įvertinimas

Bendrasis duomenų apsaugos reglamentas (BDAR) nėra vien tik IT technologijos. Kadangi dauguma duomenų yra laikoma sistemose, šios technologijos sudaro reikšmingą atitikties reglamentui dalį. Minimose sistemose duomenys, surinkti rankiniais ar automatizuotais būdais yra apdorojami, taip pat duomenys gali būti perduodami iš vienos sistemos į kitą. Reikia atsižvelgti ir į trečiųjų šalių aspektą – dabartinėse IT technologijose dirbama pasitelkiant įvairius paslaugų tiekėjus: interneto ryšio, duomenų centrų paslaugų, debesų kompiuterijos ir pan., todėl svarbu užsitikrinti tiek dokumentiškai, tiek IT ir procesų požiūriu, jog naudojamos trečiųjų šalių paslaugos taip pat atitinka BDAR reikalavimus.

Norint atitikti BDAR reikalavimus ir apsibrėžti tam būtinas organizacines ir technines priemones, reikia atlikti turimos IT infrastruktūros analizę saugumo požiūriu bei įvertinti procesus toje infrastruktūroje.

|  |  |  |
| --- | --- | --- |
| 10  **Procesų** | ~150  **Kompiuteriai** | 7  **Virtualūs serveriai** |
| 5  **Atsarginių kopijų saugyklos** | 20  **Sistemų** | 7  **Fiziniai serveriai** |

## II.2 Darbo vietos

Vadovaujantis darbuotojų atsakymais Bendrovės IT ūkį sudaro apie 150 kompiuterių. Ne visi kompiuteriai yra įmonės nuosavybė, keletas darbuotojų naudoja asmeninius kompiuterius darbo vietose.

Bendrojo duomenų apsaugos reglamento įvertinimo projekte buvo atliekama infrastruktūros analizė. Projekto metu buvo identifikuota apie 150 naudojamų kompiuterių. Kompiuterinių darbo vietų operacinių sistemų analizė buvo daroma tik „Imonė xxx“ Vilniaus miesto padalinyje, kuris įsikūręs Žirnių g. 12.

18 kompiuterių naudoja Windows 10 Home operacinę sistemą (toliau – OS), 4 naudoja Windows 10 Pro, 6 naudoja Windows 8.1 Pro. 15 Thin client naudoja Linux OS.

20 darbuotojų naudoja stacionarius kompiuterius, nešiojamų kompiuterius naudojama 28 vienetai.

Visi kompiuteriai naudoja Windows standartinę antivirusinę programą. Bendrovėje kompiuterinėms darbo centralziuotai nėra valdomos. Active Directory naudojama tik vartotojams (ang. User) kūrti. Grupinės politiko (ang. GPO) taip pat nėra naudojamos. Infrastruktūros ir darbo vietų priežiūrą vykdo „Imonė xxx“ IT padalinys.

Remiantis už IT infrastruktūrą atsakingo darbuotojo pateikta informacija, „Imonė xxx“ nekontroliuoja slaptažodžių politikos. Automatinis užsirakinimas po nustatyto periodo nekontroliuojamas. Detalesnė informacija apie prisijungimus prie sistemų yra pateikiama **Lentelėje Nr. III.2.4: Prisijungimų prie sistemų būdai.** Kompiuteriai yra ne apsaugoti nuo išorinių USB laikmenų naudojimo antivirusine sistema, taip pat yra galimybė laikmenoje esančius failus paleisti su „auto-run“ funkcija.

## II.3 Serverių infrastruktūra

Serveriai yra pagrindinis IT infrastruktūros elementas dėl savo darbo specifikos, t. y. turintys daugiausia su BDAR susijusios informacijos (asmens duomenų), todėl dažniausiai tai būna vieni iš rizikingiausių įmonės IT infrastruktūros objektų.

Duomenų vagystės atveju įsilaužimai į serverius gali turėti kur kas platesnes pasekmes, nei neleistina prieiga prie vieno ar kelių darbuotojų kompiuteriuose esančios informacijos. Todėl tinkamas serverių naudojimas ir saugumas yra labai svarbus užtikrinant bendrą IT saugą, politikų naudojimą bei atitikimą BDAR.

Bendrovė savo vidinėje infrastruktūroje turi 7 fizinius ir 7 virtualius serverius - detalesnė informacija pateikta **Lentelėje Nr. II.3.1.** **Serverių infrastruktūra**. Taip pat įmonė naudojasi 2 išoriniais sprendimais (servisais), kurie palaiko Navision ir Google docs sistemas.

Nepavyko identifikuoti visų naudojamų serverių operacinių sistemų. Įvertinimo metu nebuvo identifikuota Sugar CRM serverio operacinė sistema, kadangi visa atsakomybė yra pas sistemą prižiūrintį paslaugos teikėją.

Tik dviejų (**SRV-A** ir **TSSRV-PC1**) iš septynių fizinių serverių gamintojo garantija galioja.

Internetinės svetainės veikia išorinėse paslaugų teikėjo (angl. hosting) infrastruktūrose. UAB „Baltnetos komunikacijos“ - teikia prieglobą [www.Imonė xxx.eu](http://www.bunasta.eu) ir <http://transportoforumas.lt> svetainėms, o UAB „Interneto vizija“ teikia prieglobą <https://pagaljurgi.lt> svetainei. UAB „Imonė xxx“ prižiūri tik internetinių puslapių turinį, techninę priežiūrą atlieka trečiosios šalys UAB „We Are Marketing“ ir UAB „Artme“. Internetinės svetainės ir jų privatumo politika detaliau analizuojama **IV.2.7** skyriuje „Asmens duomenys tinklapiuose (Privatumo ir slapukų politika)“.

**Lentelė Nr. II.3.1 Serverių infrastruktūra:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Fizinis Serveris | | | | Virtualus serveris | | Sistema |
| Serverio vardas | Fizinio serverio HW | Operacinė sistema | Garantija (Ar galioja garantija serverio įrangai) | Serverio vardas | Operacinė sistema |
| TSSRV-PC | HPE ProLiant ML10 Gen9/24Gb/256SSD/6TB HDD/LAN | Windows Server 2012 R2 x64 | Ne | N/A | | Terminal server 1 |
| File Server |
| 3cx SBC |
| TSSRV-PC1 | Dell PowerEdge T430/SAS 1Gb HDD/2TB HDD/96Gb RAM/LAN | Windows Server 2012 R2 x64 | Taip | Avilda |
| Terminal server 2 |
| dcapulsepi-SRP161C3C9F9 | Raspberry Pi 3 Model B Rev 1.2 | Linux version 4.14.34-v7+ | Ne | Spausdintuvų priežiūros sistema |
| SRV-A | Synology DS218 | DSM | Taip | Archyvas |
| NAS-BCK | Netgear 250 ReadyNAS | ReadyNAS OS V6.10.0 | Ne | Atsarginės kopijos |
| VPN-SERVER | HP ProLiant MicroServer Gen8/ 320HDD/ 16Gb RAM/LAN | MS Windows 8.1 Pro x64 | Ne | VPN |
| Dahua DVR System | Dahua | Dahua | Ne | Vaizdo stebėjimas |
| N/A | | | | Hetzner (Vokietijoje) | - | Sugar CRM |
| we.Imonė xxx.eu | linux | Web Baltneta (Imonė xxx tinklapis) |
| terminalsrv | Microsoft Windows Server 2016 (64-bit) | Terminal Server 3Baltneta |
| Terminal Server 4Baltneta |
| sqlsrv | Microsoft Windows Server 2016 (64-bit) | SQL Euroskaita baltneta |
| mail.Imonė xxx.lt | linux | El.pašto sistema |
| adsrv | Microsoft Windows Server 2016 (64-bit) | Active Directory |
| Berp | Debian 10 | ERP |
| Nemokamas Google docs sprendimas (Cloud) | | Google Docs |
| Debesijos sprendimas - atsakomybė pas paslaugos teikėją (Softera) | | Navision |

## II.4 Atsarginių kopijų infrastruktūra

„Imonė xxx“ įmonės veiklos tęstinumui užtikrinti naudoja rezervinio kopijavimo sprendimus. Kaip pagrindinė atsarginio kopijavimo repozitorija yra naudojamas NAS-BCK (naudojama OS - ReadyNAS OS V6.10.0) fizinis įrenginys į kurį yra daromos bendrovės IT sistemų atsarginės kopijos. Rezervinis kopijavimas nėra taikomas keturioms sistemoms – CRM, Vaizdo stebėjimo sistemai, internetiniam puslapiui [pagaljurgi.lt](http://pagaljurgi.lt) bei spausdintuvo priežiūros sistemai, tačiau paskutinei paminėtai sistemai nėra poreikio daryti atsargines kopijas. Sistemoms, už kurias yra atsakingos trečiosios šalys atsargines kopijas, pagal pasirašytas SLA sutartis privalo užtikrinti paslaugos tiekėjas.

Atsarginių kopijų infrastruktūros detalizacija pateikiama **Lentelėje Nr. II.3.2. Atsarginių kopijų infrastruktūra.**

„Imonė xxx“ nėra apsibrėžusi kurios sistemos yra kritiškos verslo požiūriu, nėra įvertinti sistemų toleruojami neveikimo laikai (angl. recovery time objective – RTO) bei toleruojamų prarastų duomenų kiekiai (angl. recovery point objective – RPO).

**Lentelė Nr. II.4.1 Atsarginių kopijų infrastruktūra:**

|  |  |  |
| --- | --- | --- |
| **Sistemos** | **Serverių sąrašas** | **Atsarginių kopijų procesas** |
| **Microsoft Dynamics Navision** | Nuomojamas virtualus serveris | Debesijos sprendimas - atsakomybė pas paslaugos teikėją (Softera) |
| **Atsarginių kopijų sistema** | NAS-BCK | Macrium reflect programinė įranga naudojama atsarginėms kopijoms daryti. Kartą per naktį įsijungia NAS sistema, į kurią yra padaroma sistemų atsarginė kopija. Po atsarginių kopijų padarymo NAS sistema išsijungia. Kopijos yra saugomos 14 d. (2 pilnos kopijos ir 13 incremental tipo kopijų) |
| **Avilda** | TSSRV-PC1 Server |
| **Elektroninio pašto sistema** | mail.Imonė xxx.eu | Baltnet'os sprendimas. 14d. Backup 24 h RPO |
| **Vaizdo stebėjimo sistema** | Dahua DVR system | Atsarginės kopijos nedaromos |
| **CRM** | Virtualus crm-legacy.internalImonė xxx.eu | Atsarginės kopijos nedaromos |
| **Failų serveris** | TSSRV-PC | Macrium reflect programinė įranga naudojama atsarginėms kopijoms daryti. Kartą per naktį įsijungia NAS sistema, į kurią yra padaroma sistemų atsarginė kopija. Po atsarginių kopijų padarymo NAS sistema išsijungia. Kopijos yra saugomos 14 d. (2 pilnos kopijos ir 13 incremental tipo kopijų) |
| **Euroskaita** | sqlsrv | Baltnet'os sprendimas. 14d. Backup 24 h RPO |
| **ERP** | berp | Baltnet'os sprendimas. 14d. Backup 24 h RPO |
| **Google Docs** | N/A | Atsarginį kopijavimą užtikrina Google, papildomų sprendimų Imonė xxx netaiko |
| **VPN-SERVER** | VPN-SERVER | Daroma atsargine kopija daroma kas mėnesį. Pilna kopija saugoma mėnesį. |
| **Spausdintuvu priežiūros sistema** | dcapulsepi-SRP161C3C9F9 | N/A |
| **IP telefonija 3CX** | TSSRV-PC, Imonė xxx.3cxcloud.lt | Už atsargines kopijas atsako 3 šalis – „Tenesys“. Kopijos daromos kiekviena parą 12:00:00 val. |
| **Internetiniai tinklapiai (Imonė xxx.eu)** | Imonė xxx.eu | Baltnet'os sprendimas. 14d. Backup 24 h RPO |
| Kvatoklis (pagaljurgi.lt) | Atsarginės kopijos nedaromos |
| **Active directory** | adsrv | Baltnet'os sprendimas. 14d. Backup 24 h RPO |
| **Terminal Server1 (TSSRV-PC)** | TSSRV-PC | Macrium reflect programinė įranga naudojama atsarginėms kopijoms daryti. Kartą per naktį įsijungia NAS sistema, į kurią yra padaroma sistemų atsarginė kopija. Po atsarginių kopijų padarymo NAS sistema išsijungia. Kopijos yra saugomos 14 d. (2 pilnos kopijos ir 13 incremental tipo kopijų) |
| **Terminal Server2 (TSSRV-PC1)** | TSSRV-PC1 |
| **Terminal Server3 (terminalsrv)** | terminalsrv | Baltnet'os sprendimas. 14d. Backup 24 h RPO |
| **Terminal Server4 (terminalsrv)** | terminalsrv | Baltnet'os sprendimas. 14d. Backup 24 h RPO |

Bendraujant su „Imonė xxx“ atstovais bei remiantis už IT infrastruktūrą atsakingo darbuotojo pateikta informacija identifikuota, kad veiklos tęstinumui užtikrinti tarp verslo srities ir IT paslaugas teikiančių įmonių yra pasirašytos paslaugų lygių (angl. SLA) sutartys. Trečiosios šalys sutartimi privalo įsipareigoti - užtikrinti sklandų serverių veikimą, serveriuose laikomų duomenų saugumą, rezervinių kopijų darymą bei kritinių sistemų atstatomumą.

**Rekomendacija:** peržiūrėti visas turimas SLA sutartis su trečiosiomis šalimis ir įsitikinti, jog sutartyse yra:

* Įvertintas toleruojamų sistemų neveikimo laikų (angl. recovery time objective – RTO) bei toleruojamų prarastų duomenų kiekiai (angl. recovery point objective – RPO);
* Numatytos baudos, už sutartinių įsipareigojimų nevykdymą, kai sistemos neveiks ilgiau, nei tai numatyta sutarties sąlygose;
* Aiškiai apibrėžta, kokios ataskaitos ir/ar išvadas ir kokiu periodiškumu yra pateikiamos apie „Imonė xxx“ naudojamus IT servisus / infrastruktūrą.

Pažymėtina, kad atsarginių kopijų tvarka būtų suderinta su duomenų laikymo ir išsaugojimo laikotarpiais (retention policy) ir informacinės saugos politikomis, kuriose turėtų būti pateiktas maksimalus duomenų laikymo laikotarpis. Su verslu suderinti ir aprašyti duomenų atstatymo ir toleruojamų prarasti duomenų kiekius, pasirengtas ir įgyvendintas įmonės IT sistemų veiklos tęstinumo (angl. - „disaster recovery“) planas.

## II.5 Identifikuoti IT infrastruktūros faktai

**Teigiami**

* Yra naudojami ugniasienės ir VPN prisijungimo sprendimai (Saugumas);
* Yra naudojamas Terminalinių serverių sprendimas (Saugumas);
* Daugumai serverių daromos rezervinės kopijos (Valdymas);

**Neigiami**

* Kompiuterinės vietos nėra valdomas centralizuotai, centralizuotai valdoma tik vartotojų prisijungimas prie darbo vietų;
* Veiklos tęstinumui užtikrinti nėra parengto ir su verslu suderinto „disaster recovery“ plano;
* Kompiuterinis tinklas neatitinka gerųjų rekomendacijų;
* Neatliekami reguliarūs IT saugumo mokymai;
* Išmanieji įrenginiai (mobilieji telefonai, planšetės) nėra valdomi centralizuotomis priemonėmis;
* Nėra šifruojamos rezervinės duomenų kopijos, taip pat nereglamentuotas duomenų atstatymas;
* Nėra šifruojami serverių ir nešiojamų kompiuterių kietieji diskai;
* Vartotojų kompiuteriuose naudojamos administratoriaus teisės;
* Kompiuterinės darbo vietos bei serveriai galimai naudoja nelegalias antivirusines sistemas;
* Fizinių serverių (TSSRV-PC, dcapulsepi-SRP161C3C9F9, NAS-BCK, VPN-SERVER ir Dahua DVR System) techninės įrangos garantija yra pasibaigusi;
* 16 kompiuterinių darbo vietų naudoja gamintojo nebepalaikomą operacinę sistemą;
* Nėra apsirašytos slaptažodžių politikos, o naudojama dabartinė politika neatitinką geriausių rekomendacijų – slaptažodžiai yra per silpni, nėra privalomai keičiami, nėra „Lockout“ politikos bei kompiuteriuose nėra nustatytas automatinis užsirakinimas po nustatyto periodo.

**Detalus IT infrastruktūros įvertinimas pateikiamas ataskaitos priede Nr. 1**

# IT rizikų vertinimas

## III.1 Sistemų apžvalga

Bendrovė savo pagrindinėje veikloje naudoja 20 informacinių sistemų. Dalis sistemų veikia lokaliose fizinėse ir virtualizuotose aplinkose, kurių veikimą užtikrina „Imonė xxx“ IT padalinys, o likusi dalis sistemų veikia kaip SaaS ir lasS paslaugos, kurias prižiūri 3 šalys.

Detalizacija kokios trečios šalys ir prie kokių sistemų gali prisijungti iš išorės nurodyta **Lentelėje Nr. III.1.1 Informacinių technologijų (IT) sistemų sąrašas.**

**Lentelė Nr. III.1.1 Informacinių technologijų (IT) sistemų** **sąrašas**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Duomenų aplinka** | **Aprašymas** | **Vieta** | **Atsakingas skyrius** | **Vartotojų skaičius** | **Ar perduodami duomenys už EU** |
| **Microsoft Dynamics Navision** | Apskaitos bei verslo valdymo sistema | Išorinis | Buhalterija | 4 | Ne |
| **Atsarginių kopijų sistema** | Backup sprendimas | Vidinis | IT | 1 | Ne |
| **Avilda** | Muitinės programa | Išorinis | IT | 30 | Ne |
| **Elektroninio pašto sistema** | Elektroninio pašto sistema | Išorinis | IT | ~200 | Taip |
| **Vaizdo stebėjimo sistema** | Vaizdo stebėjimo sistema | Vidinis | IT | 2 | Ne |
| **CRM** | Klientų valdymo sistema | Išorinis | IT | 376 | Taip |
| **Failų serveris** | Failų saugojimo sistema | Vidinis | IT | ~160 | Taip |
| **Euroskaita** | Finansinės apskaitos sistema | Vidinis | Buhalterija | 9 | Ne |
| **ERP** | Resursų valdymo sistema. | Išorinis | IT | 2 | Taip |
| **Google Docs** | Sistema naudojama ataskaitoms talpinti (Nemokamas Google sprendimas) | Išorinis | IT | 250 | Taip |
| **VPN-SERVER** | VPN Serveris | Vidinis | IT | 17 | Ne |
| **Spausdintuvu priežiūros sistema** | Sistema skirta centralizuotai valdyti įmonės spausdintuvus | Vidinis | IT | 1 | Ne |
| **IP telefonija 3CX** | IP telefonija: Telefoninių pokalbių įrašai, IVR (tiek vidinė, tiek išorinė) | Vidinis | IT | 222 | Taip |
| **Internetiniai tinklapiai (Imonė xxx.eu)** | Internetinis tinklapis (www.Imonė xxx.eu) | Išorinis | IT | N/A | Ne |
| **Internetiniai tinklapiai (pagaljurgi.lt)** | Internetinis tinklapis (www.pagaljurgi.lt) | Išorinis | IT | N/A | Ne |
| **Active directory** | Katalogų sistema leidžianti saugoti informacija | Išorinis | IT | 46 | Ne |
| **Terminal Server1 (TSSRV-PC)** | Aplinka skirta dirbti darbuotojams nuotoliniu būdu | Vidinis | IT | 6 | Ne |
| **Terminal Server2 (TSSRV-PC1)** | Aplinka skirta dirbti darbuotojams nuotoliniu būdu | Vidinis | IT | 34 | Ne |
| **Terminal Server3 (terminalsrv)** | Aplinka skirta dirbti darbuotojams nuotoliniu būdu | Išorinis | IT | 42 | Ne |
| **Terminal Server4 (terminalsrv)** | Aplinka skirta dirbti darbuotojams nuotoliniu būdu | Išorinis | IT | 4 | Ne |

Dalis organizacijos IT sistemų veikia, kaip paslaugos, kurių veikimą ir priežiūrą užtikrina trečiosios šalys. Tokios sistemos kaip – Microsoft Dynamics Navision, El. pašto sistema, CRM, Euroskaita, ERP, Google Docs, Active directory, Terminal Server 3 ir Terminal server 4 veikia debesų kompiuterijoje kaip laaS (Infrastructure as a service) bei SaaS (software as a service) sprendimai. Kita dalis sistemų veikia lokaliose fizinėse aplinkose ir jų veikimą užtikrina „Imonė xxx“ IT skyrius.

Detalus sistemų sąrašas pateiktas **Lentelėje Nr. III.1.2. Informacinių technologijų (IT) sistemų lokacija.**

**Lentelė Nr. III.1.2 Informacinių technologijų (IT) sistemų lokacija**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sistema** | **Sistemų lokacija** | | | | **3 šalys** |
|
| **Serverio Pavadinimas** | **Tipas** | **Lokacija** | **Išorinė prieiga** |  |
| **Microsoft Dynamics Navision** | Softeros Virtuali mašina | Virtualus | laaS\*\* | Galima | UAB „Softera“ |
| **Atsarginių kopijų sistema** | NAS-BCK | Fizinis | Fizinis NAS | Negalima | - |
| **Avilda** | TSSRV-PC1 | Fizinis | Fizinis serveris | VPN | - |
| **Elektroninio pašto sistema** | mail.Imonė xxx.eu | Virtualus | Virtualizuotas "Baltnet" sprendimas | Galima | UAB "Baltneta" |
| **Vaizdo stebėjimo sistema** | Dahua DVR System | Fizinis | Fizinis PC | VPN | - |
| **CRM** | crm-legacy.internalImonė xxx.eu | Virtualus | laaS\*\* | Galima | UAB "Mokas IT" |
| **Failų serveris** | TSSRV-PC | Fizinis | Fizinis serveris | VPN | - |
| **Euroskaita** | sqlsrv | Virtualus | laaS\*\* | VPN | UAB "Baltneta" |
| **ERP** | berp | Virtualus | laaS\*\* | VPN | UAB „Baltneta“ LLC „Icode“ |
| **Google Docs** | N/A | Virtualus | SaaS\* | Galima | "Google" |
| **VPN-SERVER** | VPN-SERVER | Fizinis | Fizinis serveris | VPN | - |
| **Spausdintuvu priežiūros sistema** | dcapulsepi-SRP161C3C9F9 | Fizinis | Fizinis Raspberry Pi | Galima | UAB „4office“ |
| **IP telefonija 3CX** | TSSRV-PC | Fizinis | Fizinis serveris | Galima | UAB „Tenesys“ |
| **pagaljurgi.lt** | Kvatoklis | Virtualus | Virtualus | Galima | UAB "Interneto vizija" |
| [www.Imonė xxx.eu](http://www.bunasta.eu/) | [web.Imonė xxx.eu](http://www.bunasta.eu/) | Virtualus | Virtualus | Galima | UAB „We Are Marketing“ UAB „Baltneta“ |
| **Active directory** | adsrv | Virtualus | laaS\*\* | VPN | UAB "Baltneta" |
| **Terminal Server1 (TSSRV-PC)** | TSSRV-PC | Virtualus | Fizinis | VPN | - |
| **Terminal Server2 (TSSRV-PC1)** | TSSRV-PC1 | Virtualus | Fizinis | VPN | - |
| **Terminal Server3 (terminalsrv)** | terminalsrv | Virtualus | laaS\*\* | VPN | UAB "Baltneta" |
| **Terminal Server4 (terminalsrv)** | terminalsrv | Virtualus | laaS\*\* | VPN | UAB "Baltneta" |

\* SaaS – Programinė įranga kaip paslauga (angl. software as a service)

\*\* IaaS – Infrastruktūra kaip paslauga (angl. infrastructure as a service)

Visose sistemose išskyrus Atsarginių kopijų sistemoje yra pradėta konfigūruoti galimybė jungtis išoriniams paslaugų teikėjams arba paslaugų gavėjams. Iš naudojamų 20 sistemų, 11 turi VPN jungimosi galimybę. VPN naudojamas **tik prisijunti prie Bendrovės vidinio tinklo**, iš kurio jau įprastai jungiamasi prie sistemų. VPN sprendimas nėra niekaip loginamas ir nėra užtikrinama prisijungimų atsekamumas.

## III.2 Sistemų rizikų vertinimas

**Situacija**

BDAR teigia (II skyrius, 5 skirsnis), jog duomenys turi būti apdorojami užtikrinant tinkamą saugumo lygį. Tokį saugumo lygį turi padėti užtikrinti taikomos saugumo priemonės. Į šių priemonių kompleksą įeina tiek techninės (programinė bei aparatinė įranga), tiek ir organizacinės priemonės (politikos bei procesai). Tam, kad nustatytume gaires į ką pirmiausia reiktų atkreipti dėmesį, atlikome Jūsų sistemų rizikų įvertinimą.

Bendras sistemų rizikingumas **Lentelė Nr. III.2.1: Duomenų pažeidimų rizikos įvertinimas pagal sistemas** buvo atliktas vertinant pagal penkis skirtingus kriterijus, kurie parteikti **LENTELĖJE NR. III.2.1.1: BDAR RIZIKINGUMO VERTINIMAS.**

**Lentelė Nr. III.2.1: Duomenų pažeidimų rizikos įvertinimas pagal sistemas:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sistema** | **Vartotojų skaičius** | **Ar duomenys perduodami už EU ribų** | **Partneriai kurie jungiasi prie sistemų** | **Rizikos balas** |
| Microsoft Dynamics Navision | 4 | Ne | UAB „Softera“ | 10,5 |
| Atsarginių kopijų sistema | 1 | Ne | - | 10 |
| Avilda | 30 | Taip | - | 10 |
| Elektroninio pašto sistema | ~200 | Taip | UAB „Baltneta“ | 10,5 |
| Vaizdo stebėjimo sistema | 2 | Ne | - | 5 |
| CRM | 376 | Taip | UAB „Mokas IT“ ir laisvai samdomi darbuotojai (angl. Freelancer) | 10,5 |
| Failų serveris | ~160 | Taip | - | 10,5 |
| Euroskaita | 9 | Ne | UAB „Proto technika“ | 10,5 |
| ERP | 2 | Taip | UAB „Baltneta“  LLC „Icode“ | 10.5 |
| Google Docs | 250 | Taip | PL, LV, BY, RU biurų darbuotojai, kurie jungiasi per terminalinį serverį | 8 |
| VPN-SERVER | 17 | Ne | - | 5,5 |
| Spausdintuvu priežiūros sistema | 1 | Ne | UAB „4office“ | 6 |
| IP telefonija 3CX | 222 | Taip | UAB „Tenesys“ | 6,5 |
| Internetiniai tinklapiai (Imonė xxx.eu) | N/A | Ne | UAB „We Are Marketing“  UAB „Baltneta“ | 5 |
| Internetiniai tinklapiai (pagaljurgi.lt) | N/A | Ne | - | 5 |
| Active directory | 46 | Ne | UAB „Baltneta“ | 7 |
| Terminal Server1 (TSSRV-PC) | 6 | Ne | UAB „Baltneta“ | 7 |
| Terminal Server2 (TSSRV-PC1) | 34 | Ne | UAB „Baltneta“ | 6,5 |
| Terminal Server3 (terminalsrv) | 42 | Ne | UAB „Baltneta“ | 6,5 |
| Terminal Server4 (terminalsrv) | 4 | Ne | UAB „Baltneta“ | 6,5 |

|  |  |  |
| --- | --- | --- |
| Žema | Vidutinė | Aukšta |
| 4 5 6 | 7 8 9 | 10 11 12 |

Rizikos balas yra gaunamas iš žemiau pateiktos lentelės (Sistemos rizikingumas ir Duomenų srautas sistemose):

**Lentelė Nr. III.2.1.1: BDAR rizikingumo vertinimas:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Rizikos objektas** | **Sistemos įvertinimas** | **Sistemų rizikingumas** | **Duomenų srautas sistemose** |
| **Microsoft Dynamics Navision** | 10.5 | 9 | 12 |
| **Atsarginių kopijų sistema** | 10 | 8 | 12 |
| **Avilda** | 10 | 9 | 11 |
| **Elektroninio pašto sistema** | 10.5 | 10 | 11 |
| **Vaizdo stebėjimo sistema** | 5 | 6 | 4 |
| **CRM** | 10.5 | 10 | 11 |
| **Failų serveris** | 10.5 | 9 | 12 |
| **Euroskaita** | 10.5 | 9 | 12 |
| **ERP** | 10.5 | 10 | 11 |
| **Google Docs** | 8 | 8 | 8 |
| **VPN-SERVER** | 5.5 | 7 | 4 |
| **Spausdintuvu priežiūros sistema** | 6 | 8 | 4 |
| **IP telefonija 3CX** | 6.5 | 8 | 5 |
| **Internetiniai tinklapiai (Imonė xxx.eu)** | 5 | 6 | 4 |
| **Internetiniai tinklapiai (pagaljurgi.lt)** | 5 | 6 | 4 |
| **Active directory** | 7 | 8 | 6 |
| **Terminal Server1 (TSSRV-PC)** | 7 | 9 | 5 |
| **Terminal Server2 (TSSRV-PC1)** | 6.5 | 8 | 5 |
| **Terminal Server3 (terminalsrv)** | 6.5 | 8 | 5 |
| **Terminal Server4 (terminalsrv)** | 6.5 | 8 | 5 |

Sistemos įvertinimas yra gaunamas iš šių stulpeliu Sistemų rizikingumas ir Duomenų srauto sistemose balų vidurkio. Sistemų rizikingumo balas detaliau aprašytas **Lentelėje Nr. III.2.5: Rizikingumo vertinimas pagal skirtingus Kriterijus**, o Duomenų srautas sistemose balas aprašytas **Lentelė Nr. III.2.1.2: Duomenų srautas sistemose.**

**Lentelė Nr. III.2.1.2: Duomenų srautas sistemose:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sistema** | **Kiekis skirtingų duomenų tipų** | **Jautrumas** | **Apimtis** | **Duomenų aplinkos jautrumas** | **Bendra rizika** |
| **Microsoft Dynamics Navision** | Nuo 20 | Taip | Nuo 10000 | Aukštas | 12 |
| **Atsarginių kopijų sistema** | Nuo 20 | Taip | Nuo 10000 | Aukštas | 12 |
| **Avilda** | Nuo 20 | Taip | Nuo 10000 | Vidutinis | 11 |
| **Elektroninio pašto sistema** | Nuo 20 | Taip | Nuo 10000 | Vidutinis | 11 |
| **Vaizdo stebėjimo sistema** | Nuo 1 iki 4 | Ne | Nuo 1 iki 500 | Žemas | 4 |
| **CRM** | Nuo 20 | Taip | Nuo 10000 | Vidutinis | 11 |
| **Failų serveris** | Nuo 20 | Taip | Nuo 10000 | Aukštas | 12 |
| **Euroskaita** | Nuo 20 | Taip | Nuo 10000 | Aukštas | 12 |
| **ERP** | Nuo 20 | Taip | Nuo 10000 | Vidutinis | 11 |
| **Google Docs** | Nuo 20 | Ne | Nuo 2000 iki 10000 | Vidutinis | 8 |
| **VPN-SERVER** | Nuo 1 iki 4 | Ne | Nuo 1 iki 500 | Žemas | 4 |
| **Spausdintuvu prieziuros sistema** | Nuo 1 iki 4 | Ne | Nuo 1 iki 500 | Žemas | 4 |
| **IP telefonija 3CX** | Nuo 4 iki 10 | Ne | Nuo 1 iki 500 | Žemas | 5 |
| **Internetiniai tinklapiai (Imonė xxx.eu)** | Nuo 1 iki 4 | Ne | Nuo 1 iki 500 | Žemas | 4 |
| **Internetiniai tinklapiai (pagaljurgi.lt)** | Nuo 1 iki 4 | Ne | Nuo 1 iki 500 | Žemas | 4 |
| **Active directory** | Nuo 4 iki 10 | Ne | Nuo 500 iki 2000 | Žemas | 6 |
| **Terminal Server1 (TSSRV-PC)** | Nuo 4 iki 10 | Ne | Nuo 1 iki 500 | Žemas | 5 |
| **Terminal Server2 (TSSRV-PC1)** | Nuo 4 iki 10 | Ne | Nuo 1 iki 500 | Žemas | 5 |
| **Terminal Server3 (terminalsrv)** | Nuo 4 iki 10 | Ne | Nuo 1 iki 500 | Žemas | 5 |
| **Terminal Server4 (terminalsrv)** | Nuo 4 iki 10 | Ne | Nuo 1 iki 500 | Žemas | 5 |

Įvertinimo metu gauti duomenys leidžia teigti, kad iš IT pusės dideles rizikas turi tos sistemos, kuriuose yra didelis kiekis asmens duomenų. Nors didžiausias rizikas pagal duomenų pažeidimų rizikos įvertinimą turi aštuonios iš dvidešimt sistemų: Microsoft Dynamic Navision, Atsarginių kopijų, Avilda, Elektroninio pašto, CRM, Failų serveris, Euroskaita, ERP. Tačiau pagal duomenų aplinkos jautrumą sistemose pirmiausia dėmesį reiktų atkreipti į: El. pašto, Microsoft Dynamics Navision, Euroskaita, Failų serverį ir Atsarginių kopijų sistemas.

Planuojant IT investicijas ar vykdant įmonės veiklos tęstinumo užtikinimo (angl. disaster recovery) planą ir siekiant didinti sistemų patikimumą rekomenduojame neišskirti nei vienos sistemos ir kreipti dėmesį į visas turimas sistemas, nebent verslo poreikiai būtų kitokie.

Pagal saugomų asmens duomenų tipus ir kiekius (**Lentelė Nr. III.2.2.: Sistemose saugomų asmens duomenų tipai**) dauguma Bendrovės sistemų saugo tipinius asmens duomenis (vardas, pavardė, padalinys, pareigos, nuotrauka, el. p. adresas, asmens profesiniai duomenys). Didžiausias asmens duomenų kiekis yra – Microsoft Dynamics Navision, Avilda, Elektroninio pašto sistema, CRM, Euroskaita, ERP, Failų serverį ir Atsarginių kopijų sistemose. Būtent šiose sistemose saugomas didžiausias asmens duomenų kiekis tiek pagal jų tipus, tiek ir pagal apimtį.

Atkreipiamas dėmesys, kad audito metu nepavyko susipažinti su visų sistemų detaliais procesų aprašymais ir dokumentacija. Buvo identifikuotos septyniolika iš dvidešimt sistemų, kokie asmens duomenys sistemose yra laikomi, tačiau tikslių saugojimo terminų, duomenų naikinimo tvarkų ir aprašų, bei duomenų kategorizavimo nebuvo identifikuota. Esant visiems aukščiau paminėtiems kriterijams bendras sistemų rizikingumo rodiklis būtų mažesnis. Ši pastaba ypač aktuali aukščiau išvardintoms sistemoms, kuriose yra didelis duomenų kiekis arba saugomi jautrūs duomenys, t. y. didelė asmens duomenų koncentracija.

**Lentelė Nr. III.2.2: Sistemose saugomų asmens duomenų tipai.**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Sistema** | **Asmens duomenys** | | | | | | | | | |
| **Identifikatoriai** | | | **Profiliavimo duomenys** | | | | | | **Stebėjimas** |
| Asmens | Technologiniai | Biometriniai / Genetiniai | Netiesioginiai | Finansiniai | Socialiniai | Išoriniai | Sveikatos | Fiziniai | Video |
| **Microsoft Dynamics Navision** | Vardas, pavardė | El. paštas, telefonas | - | - | Sąskaitos numeris | Asmens profesiniai duomenys | Pomėgiai | - | Amžius, Lytis | - |
| **Atsarginių kopijų sistema** | Vardas, pavardė, El. paštas, AD ID | El. paštas, telefonas | Pareigos, Balso įrašymas | Gyv. vietos adresas, Automobilio valst. Nr., Darbo vietos adresas, vairuotojo pažymėjimo kortelės numeris, Vilkiko numeris, priekabos numeris, EPI numeris, paslaugos tipas(krovinio vertė, mokesčių suma), Skyrius/miestas, kuriame dirba žmogus, | Sąskaitos numeris | Asmens profesiniai duomenys, Šeimyninė padėtis ir šeimyninė sudėtis, CV dokumentai, Kriminalinė informacija, Asmens profesiniai duomenys, | Turimos vairuotojo kategorijos, Pomėgiai | Sveikatos duomenys | Amžius, Lytis | Nuotraukos, vaizdo įrašai |
| **Avilda** | Vardas, pavardė | El. paštas, telefonas | - | Darbo vietos adresas | - | - | - | - | - | Vaizdo įrašai |
| **Elektroninio pašto sistema** | Vardas, pavardė | El. paštas | Pareigos | Darbo vietos adresas, vairuotojo pažymėjimo kortelės numeris | - | Šeimyninė padėtis ir šeimyninė sudėtis, CV dokumentai, Kriminalinė informacija | Turimos vairuotojo kategorijos | Sveikatos duomenys | - | Nuotraukos |
| **Vaizdo stebėjimo sistema** | - | - | - | - | - | - | - | - | - | Nuotraukos, vaizdo įrašai |
| **CRM** | Vardas, pavardė | El. paštas, telefonas | - | Vilkiko numeris, priekabos numeris, EPI numeris, paslaugos tipas(krovinio vertė, mokesčių suma) | - | - | - | - | - | - |
| **Failų serveris** | Vardas, pavardė, gimimo data, asmens kodas | El. paštas, telefonas | Pareigos | Gyv.viet. Adresas, Padalinys | Sąskaitos numeris | - | - | - | - | Nuotraukos |
| **Euroskaita** | Vardas, Pavarde | El.paštas | - | - | Sąskaitos numeris | CV dokumentai | Pomėgiai | - | - | - |
| **ERP** | Vardas, Pavarde | El. paštas, telefonas | Pareigos | Skyrius/miestas, kuriame dirba žmogus | Sąskaitos numeris | Asmens profesiniai duomenys | - | - | - | - |
| **Google Docs** | Vardas, pavardė | El. paštas, telefonas | - | Vilkiko numeris, priekabos numeris | - | Šeimyninė padėtis ir šeimyninė sudėtis, CV dokumentai, Kriminalinė informacija | Turimos vairuotojo kategorijos | Sveikatos duomenys | - | Nuotraukos |
| **VPN-SERVER** | Vardas, Pavardė | - | - | - | - | - | - | - | - | - |
| **Spausdintuvu priežiūros sistema** | - | El. paštas | - | - | - | - | - | - | - | - |
| **IP telefonija 3CX** | Vardas, Pavardė | El. paštas, telefonas | Balso įrašymas | Skyrius/miestas, kuriame dirba žmogus | - | - | - | - | - | - |
| **Internetiniai tinklapiai (Imonė xxx.eu)** | Vardas, Pavardė | El. paštas, telefonas | Pareigos | Skyrius/miestas, kuriame dirba žmogus | - | - | - | - | - | Nuotraukos |
| **Internetiniai tinklapiai (pagaljurgi.lt)** | Vardas, Pavardė | El. paštas | - | - | - | - | - | - | - | Nuotraukos |
| **Active directory** | Vardas, pavardė | El. paštas, telefonas | Pareigos | Skyrius/miestas, kuriame dirba žmogus | - | - | - | - | - | - |
| **Terminal Server1 (TSSRV-PC)** | Vardas, Pavardė | El. paštas, telefonas | - | Skyrius/miestas, kuriame dirba žmogus | - | - | - | - | - | - |
| **Terminal Server2 (TSSRV-PC1)** | Vardas, Pavardė | El. paštas, telefonas | - | Skyrius/miestas, kuriame dirba žmogus | - | - | - | - | - | - |
| **Terminal Server3 (terminalsrv)** | AD ID | El. paštas, telefonas | - | Skyrius/miestas, kuriame dirba žmogus | - | - | - | - | - | - |
| **Terminal Server4 (terminalsrv)** | AD ID | El. paštas, telefonas | - | Skyrius/miestas, kuriame dirba žmogus | - | - | - | - | - | - |

|  |  |
| --- | --- |
|  | Galimybė pateikti užklausa, kurioje gali būti nestruktūrizuoti asmens duomenys |
|  | Nestruktūrizuoti duomenys, kurių paieškos nėra galimybės užtikrinti automatinėmis priemonėmis. |

IT sistemose labai svarbu ne tik sistemos saugumas, bet ir jos valdymas bei funkcionalumas. Esant dideliam sistemos vartotoju kiekiui stipriai išauga žmogiškojo faktoriaus rizikos susijusios su duomenų praradimu, sugadinimu ar nesankcionuota prieiga. Todėl sistemos, kuriose yra laikomas didelis duomenų kiekis, o ypač kai tie duomenys yra priskiriami jautrių asmens duomenų kategorijai, privalo turėti automatinės duomenų paieškos, laikymo trukmės nustatymo, ištrynimo ar klasifikavimo funkcijas, jei šios sistemos buvo sukurtos, po BDAR įsigaliojimo datos. Nors “Imonė xxx” naudojamos IT Sistemos ir buvo sukurtos bei pradėtos naudoti dar iki BDAR įsigaliojimo (aukščiau paminėti sistemų reikalavimai nėra privalomi), tačiau labai rekomenduotina įsivertinti galimybę atlikti sistemų atnaujinimus, kurių metu būtų įdiegtos galimybės: atlikti asmens duomenų paiešką, ištrini duomenis automatinėmis priemonėmis, klasifikuoti asmens duomenis ir pažymėti duomenų laikymo trukme. Šie pakeitimai nėra privalomi, bent jau tol kol nėra atliekamas bet koks rimtas sistemos modifikavimas ar atnaujinimas, jei visgi sistemos atnaujinimas atliekamas - aukščiau paminėti punktai tampa privalomais.

**Lentelėje NR. III.2.3.: Sistemų atitikimas BDAR rekomendacijoms**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sistema** | **Vartotojų skaičius** | **Atsakingas skyrius** | **Galimybė atlikti asmens duomenų paiešką** | **Galimybė ištrinti duomenis automatinėmis priemonėmis** | **Galimybė klasifikuoti duomenis** | **Galimybė pažymėti duomenų laikymo trukmę** |
| Microsoft Dynamics Navision | 6 | Buhalterija | Taip | Ne | Ne | Dalinai |
| Atsarginių kopijų sistema | 1 | IT | Ne | Taip | Ne | Taip |
| Avilda | 30 | IT | Taip | Ne | Ne | Ne |
| Elektroninio pašto sistema | ~200 | IT | Dalinai | Ne | Ne | Ne |
| Vaizdo stebėjimo sistema | 2 | IT | Ne | Taip | Ne | Taip |
| CRM | 376 | IT | Dalinai | Dalinai | Ne | Ne |
| Failų serveris | ~160 | IT | Dalinai | Taip | Ne | Ne |
| Euroskaita | 9 | Buhalterija | Taip | Taip | Taip | Ne |
| ERP | 2 | IT | Ne | Ne | Ne | Ne |
| Google Docs | 250 | IT | Taip | Taip | Taip | Taip |
| VPN-SERVER | 17 | IT | Ne | Taip | Ne | Taip |
| Spausdintuvu priežiūros sistema | 1 | IT | Ne | Ne | Ne | Ne |
| IP telefonija 3CX | 222 | IT | Dalinai | Taip | Ne | Ne |
| Internetiniai tinklapiai (Imonė xxx.eu) | - | IT | N/A | N/A | N/A | N/A |
| Internetiniai tinklapiai (pagaljurgi.lt) | - | IT | N/A | N/A | N/A | N/A |
| Active directory | 46 | IT | Taip | Taip | Ne | Dalinai |
| Terminal Server1 (TSSRV-PC) | 6 | IT | Taip | Taip | Ne | Dalinai |
| Terminal Server2 (TSSRV-PC1) | 34 | IT | Taip | Taip | Ne | Dalinai |
| Terminal Server3 (terminalsrv) | 42 | IT | Taip | Taip | Ne | Dalinai |
| Terminal Server4 (terminalsrv) | 4 | IT | Taip | Taip | Ne | Dalinai |
|  |  |  |  |  |  |  |

**Prisijungimai prie sistemų**

**Lentelė Nr. III.2.4: Prisijungimų prie sistemų būdai.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sistema** | **Kokiu būdu vartotojai jungiasi prie sistemos** | | |
| **AD vartotoju / Lokaliu vartotoju** | **Jei lokaliu, tai kokiais duomenimis (pvz: Vartotojo vardas ir slaptažodis)** | **Ar naudojamas SSO (Taip/Ne)** |
| **Microsoft Dynamics Navision** | lokaliu | Vardas ir slaptažodis | Ne |
| **Atsarginių kopijų sistema** | lokaliu | Vardas ir slaptažodis | Ne |
| **Avilda** | lokaliu | Vardas ir slaptažodis | Ne |
| **Elektroninio pašto sistema** | lokaliu | Vardas ir slaptažodis | Ne |
| **Vaizdo stebėjimo sistema** | lokaliu | Vardas ir slaptažodis | Ne |
| **CRM** | lokaliu | Vardas ir slaptažodis | Ne |
| **Failų serveris** | lokaliu | Vardas ir slaptažodis | Ne |
| **Euroskaita** | lokaliu | Vardas ir slaptažodis | Ne |
| **ERP** | lokaliu | Vardas ir slaptažodis | Ne |
| **Google Docs** | lokaliu | Vardas ir slaptažodis | Ne |
| **VPN-SERVER** | lokaliu | Vardas ir slaptažodis | Ne |
| **Spausdintuvu priežiūros sistema** | - | pin | Ne |
| **IP telefonija 3CX** | lokaliu | pin ir slaptažodis | Ne |
| **Internetiniai tinklapiai (Imonė xxx.eu)** | lokaliu | Vardas ir slaptažodis | Ne |
| **Internetiniai tinklapiai (pagaljurgi.lt)** | lokaliu | Vardas ir slaptažodis | Ne |
| **Active directory** | AD vartotoju | AD/id ir slaptažodis | Ne |
| **Terminal Server1 (TSSRV-PC)** | lokaliu | Vardas ir slaptažodis | Ne |
| **Terminal Server2 (TSSRV-PC1)** | lokaliu | Vardas ir slaptažodis | Ne |
| **Terminal Server3 (terminalsrv)** | AD vartotoju | AD/id ir slaptažodis | Ne |
| **Terminal Server4 (terminalsrv)** | AD vartotoju | AD/id ir slaptažodis | Ne |

Analizuojant sistemų saugumą iš prisijungimo prie sistemų galimybių pusės **Lentelė Nr. III.2.4: Prisijungimų prie sistemų būdai.** prie 3 iš 20 sistemų yra jungiamasi per centralizuotai valdomas vartotojų paskyras (pvz.: Active Directory), kas neleidžia užtikrinti aukštesnio sistemų prieigos patikimumo. Prie 16 iš 20 sistemų jungiamasi lokalia vartotojo paskyra (vartotojo vardu ir slaptažodžiu apsaugota paskyra), bet jos valdomos atskirai kiekvienoje iš sistemų, kas ne visada leidžia užtikrinti, kad nebedirbančių ar nebevykdančių veiklos darbuotojų prieigos paskyros būtų laiku panaikintos. Spausdintuvų priežiūros sistemoje yra nustatytas PIN kodas tik keliems asmenims, todėl rekomenduojame PIN kodu apsaugotą spausdinimo funkcionalumą pritaikyti visiems organizacijos darbuotojams, kad spausdinamas dokumentas nepatektų kitam asmeniui.

**Rizikos vertinimas**

IT sistemų rizikų vertinimas buvo atliktas sistemas vertinant pagal penkis skirtingus kriterijus:

* IT/Tinklas;
* Procesai;
* Žmogiškasis faktorius;
* Verslo rizika;
* BDAR rizika.

Kiekvienas iš šių kriterijų rizikingumas yra vertinimas balais nuo 1 iki 3 (žema rizika – aukšta rizika) Duomenys gauti šios analizės metu **Lentelė Nr. III.2.5: Rizikingumo vertinimas pagal skirtingus kriterijus** kartu įvertinant ir sistemose esančius asmens duomenų kiekius buvo panaudoti įvertinti bendrą sistemos rizikingumą, kuris pateiktas **Lentelėje Nr. III.2.1: Duomenų pažeidimų rizikos įvertinimas pagal sistemas.**

**Lentelė Nr. III.2.5: Rizikingumo vertinimas pagal skirtingus Kriterijus.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sistemos** | **Vertinimas** | | | | |
| **IT/Tinklas** | **Procesai** | **Žmogiškasis faktorius** | **Verslo rizika** | **BDAR rizika** |
| Microsoft Dynamics Navision | 1 | 3 | 3 | 2 | 3 |
| Atsarginių kopijų sistema | 2 | 3 | 2 | 1 | 3 |
| Avilda | 1 | 3 | 2 | 3 | 2 |
| Elektroninio pašto sistema | 1 | 3 | 3 | 3 | 3 |
| Vaizdo stebėjimo sistema | 1 | 3 | 1 | 1 | 2 |
| CRM | 1 | 3 | 3 | 3 | 3 |
| Failų serveris | 1 | 3 | 2 | 3 | 3 |
| Euroskaita | 1 | 3 | 3 | 2 | 3 |
| ERP | 1 | 3 | 3 | 3 | 3 |
| Google Docs | 2 | 3 | 1 | 3 | 2 |
| VPN-SERVER | 1 | 3 | 1 | 2 | 2 |
| Spausdintuvų priežiūros sistema | 1 | 3 | 1 | 3 | 2 |
| IP telefonija 3CX | 1 | 3 | 1 | 3 | 2 |
| Internetiniai tinklapiai (Imonė xxx.eu) | 1 | 3 | 1 | 1 | 2 |
| Internetiniai tinklapiai (pagaljurgi.lt) | 1 | 2 | 1 | 1 | 2 |
| Active directory | 1 | 3 | 1 | 3 | 2 |
| Terminal Server1 (TSSRV-PC) | 1 | 3 | 2 | 3 | 2 |
| Terminal Server2 (TSSRV-PC1) | 1 | 3 | 2 | 2 | 2 |
| Terminal Server3 (terminalsrv) | 1 | 3 | 1 | 3 | 2 |
| Terminal Server4 (terminalsrv) | 1 | 3 | 1 | 3 | 2 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Maža tikimybė |  |  | Vidutinė tikimybė |  |  | Aukšta tikimybė |

Didžiausia rizikos tikimybė įvykti duomenų praradimui ar pažeidimui yra:

* **IT/Tinklo rizika** – santykinai žema, kadangi „Imonė xxx“ yra pakankamai gerai struktūrizavę ir apsaugoję savo IT ir tinklo infrastruktūrą, todėl nėra nei vieno išskirtinai aukštos rizikos sistemos.

Dar labiau mažinti rizikas siūlome koreguoti ir papildyti Sistemų paslaugų lygio (angl. SLA) sutartis. Taip pat rekomenduojame apsirašyti ne tik įmonės sistemų procesus, bet ir IT tinklo infrastruktūrą.

* **Procesai** – Šioje kategorijoje 8 sistemos yra aukštos rizikos - Microsoft Dynamic Navision, Avilda, Elektroninio pašto sistema, CRM, Failų serveris, Euroskaita, ERP, Google Docs. Šiose sistemoms trūksta dokumentacijos ir sistemų apsirašymo.

Mažinti šias rizikas siūlome peržiūrint veiklos procesus, mokant darbuotojus tinkamai naudotis sistemomis, įmonės viduje pasitvirtinti procedūrą kaip ir kokie dokumentai saugomi, kaip jais dalinamasi ir kada jie yra trinami. Užtikrinant, kad ir kompiuterinėse darbo vietose esanti informacija butų saugoma į rezervines kopijas.

* **Žmogiškasis faktorius** – pagal rizikingumą labiausiai rizikinga atrodo Elektroninio pašto sistema, Microsoft Dynamic Navision, CRM, Euroskaita, ERP. Prie sistemų, kurios jautrios žmogiškojo faktoriaus klaidoms, būtina paminėti tas, kuriose saugumas didžiausias asmens duomenų kiekis, t.y. Atsarginių kopijų sistema ir Failų serveris.

Mažinti šias rizikas efektyviausiai galima diegiant tinkamas organizacines priemones, pvz.: IT saugumo mokymai, konfidencialumo susitarimai, mokymai BDAR temomis, mokymai dėl saugaus pašto naudojimo, informacinių pranešimų „mailing tips“ diegimo (informuoja vartotoją pvz. apie tai, kad siunčia laišką į išorę) Pastebėtina jog rizikos gali būti susijusios tiek su darbuotojų neatsargumu, tiek su tyčine veikla – įmanomos situacijos, kai rizikos kyla iš vidaus, t.y. tyčinės darbuotojų veiklos. Papildomai rizikas galima mažinti suskirsčius darbuotojų prieigų teises prie sistemose esančių duomenų, kad darbuotojas galėtu pasiekti tik jam reikalingą ir su jo darbo pareigomis susijusią informaciją.

* **Verslo rizika** – pagal rizikingumą labiausiai rizikinga atrodo Avilda, Elektroninis paštas, CRM, Failų serveris, RPM, Google Docs, IP telefonija, Active Directory, Terminal Server 1, Terminal Server 3 ir Terminal Server 4.

Verslo rizikos, sistemos, kurių netinkama veikla turėtų didžiausią reikšmę įmonės veiklai ir jos rezultatams ilgalaikėje perspektyvoje. Šios rizikos turi būti mažinamos atliekant sistemų „disaster recovery“ plano parengimą ir įgyvendinimą arba kaip minimum užtikrinant aukštą sistemų patikimumą, ką galima būtų įgyvendinti pasinaudojant debesų kompiuterijos sprendimais.

* **BDAR rizika** – BDAR rizikos sistemos yra Elektroninio pašto sistema, CRM ir ERP.

Tai rizikos susijusios asmens duomenų kiekiu sistemose, kuo duomenų sistemoje daugiau ir kuo didesnis vartotojų kiekis, tuo rizika didesnė. Mažinti rizikas galima užtikrinant sistemų atitikimą „Privacy by Design“ principams, šviečiant ir edukuojant darbuotojus, kaip tinkamai reikia elgtis su asmens duomenimis, t.y. nerinkti ir nekaupti perteklinių duomenų, turėti teisėtus surinktų duomenų saugojimo pagrindus, užtikrinti, kad duomenys atėjus laikui būtų automatiškai šalinami iš sistemų ir pan.

## IV.3 Sistemų atitikimas gerosiomis praktikomis

Reglamentas nurodo, kad naujosios sistemos turės atitikti standartizuotosios ir numatytosios duomenų apsaugos reikalavimus. Toks atitikimas padės ateityje geriau įgyvendinti asmens duomenų teises. Ir nors šie reikalavimai nėra privalomi sistemos įdiegtoms iki įsigaliojant Reglamentui, esamų sistemų pasiruošimas ir atitikimas Reglamento nuostatomis leistų greičiau ir tiksliau suklasifikuoti duomenis bei leistų greičiau supažindinti asmenis su jų teisėmis arba įgyvendinti teisę būti pamirštam.

Vadovaujantis Valstybinės duomenų apsaugos inspekcijos parengtomis „Tinkamų organizacinių ir techninių duomenų saugumo priemonių įgyvendinimo gairėmis asmens duomenų valdytojams ir tvarkytojams“ “Imonė xxx” atitikties įvertinimas pateiktas Lentelėse Nr. IV.3.1. ir IV.3.2 **Bendrovės taikomų priemonių atitiktis VDAI rekomenduojamų 20 minimalių reikalavimų.**

**Dešimt minimalių reikalavimų dėl tinkamų techninių duomenų saugumo priemonių:**

**Lentelė Nr. IV.3.2. 10 minimalių reikalavimų dėl techninių duomenų saugumo priemonių**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Reikalavimas** | **Paaiškinimas** | **Taip/Ne (V/X)** |
| 1. | Prieigų kontrolė ir autentifikavimas | Visiems IT sistemos naudotojams taikoma Prieigų kontrolės sistema turi leisti kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras. Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir slaptažodis. | Iš dalies |
| 2. | 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. | Iš dalies |
| 3. | 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. | Iš dalies |
| 4. | Darbo stočių apsauga | Kompiuterizuotų darbo vietų naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti saugos nustatymų. | **X** |
| 5. | 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). | **V** |
| 6. | 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. | Iš dalies |
| 7. | Mobilieji, nešiojami įrenginiai | Mobiliųjų ir nešiojamų įrenginių administravimo procedūros privalo būti nustatytos ir dokumentuotos. Mobilieji, nešiojami įrenginiai turi būti užregistruoti ir autorizuoti, bei būti adekvataus prieigos kontrolės procedūrų lygio. | Iš dalies |
| 8. | Programinės įrangos sauga | Informacinėse sistemose naudojama programinė įranga turi atitikti programinės įrangos saugos gerąją praktiką, programinės įrangos kūrimo struktūras, standartus. Specifiniai saugos reikalavimai turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose. | **X** |
| 9. | Duomenų naikinimas, šalinimas | Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinti visi joje esantys duomenys, naudojant tam skirtą programinę įrangą. Tais atvejais, kai to padaryti neįmanoma, 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. | Iš dalies |
| 10. | Fizinė sauga | Turi būti įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos. | **X** |

# V. Rekomendacijos

Šiame skyriuje pateikiame svarbiausias rekomendacijas apimančias skirtingas organizacijos sritis ir veiklos sferas (IT infrastruktūrą bei vidinius procesus). Rekomendacijos buvo paruoštos taip, kad rekomendacijų įgyvendinimo rezultatas padėtų pakelti bendrą IT brandos bei vidinių verslo procesų lygį.

## V.1 IT sistemų ir procesų rekomendacijos:

|  |
| --- |
| **#1 Sukurti galimų duomenų pažeidimų valdymo planą**  Pagal BDAR, duomenų pažeidimo eskalavimui yra skirtos 72 valandos. Per šį laiką reikia ne tik sustabdyti duomenų pažeidimą, bet ir nuspręsti, ką informuoti (duomenų apsaugos inspekciją ir/ar duomenų subjektus). |
| **#2 Sukurti ir įsidiegti sistemų „disaster recovery“ planą**  Veiklos užtikrinimo tęstinumui užtikrinti, parengti ir su verslu suderinti „disaster recovery“ planą, kuriame būtų numatyti kritinių sistemų RPO ir RTO laikai, dokumentuota sistemų atstatymo procedūra. Faktiškai įgyvendinti ir IT priemonėmis užtikrinti, kad „disaster recovery“ planas būtų periodiškai išbandomas; |
| **#3 Užtikrinti fizinės IT įrangos (serverių, komutatorių) tinkamą apsaugą ir ribotą prieigą**  Jeigu nėra galimybės serverio įrengti tam dedikuotoje patalpoje, užtikrinti, kad jis būtų rakinamas komutacinėje spintoje, o raktai būtų ribotos prieigos. |
| **#4 Sumažinti rezervinio kopijavimo sistemos riziką ir apsirašyti rezervinio kopijavimo procesą**   1. Užtikrinti, kad saugomos rezervinės kopijos būtų šifruojamos; 2. Įgyvendinti rezervinio kopijavimo sprendimus, užtikrinant, kad visoms Bendrovės sistemoms būtų atliekamas rezervinis kopijavimas. |
| **#5 Užtikrinti fizinės serverinės įrangos garantinį palaikymą**  5 iš 7 fizinių serverių neturi galiojančios gamintojo garantijos. Sugedus negarantiniam serveriui yra didelė rizika, kad sistemos veikimas gali būti sutrikdytas ilgam laikui, nes negarantinės įrangos atsarginių dalių tiekimo gamintojai neįsipareigoja atlikti remonto „next business day“ ar bet kokiu kitu terminu. Rekomendacija pratęsti garantijas negarantinei įrangai, o jeigu ji jau morališkai pasenusi ir pratęsimas nėra tikslingas – pakeisti nauja, garantiją turinčia įranga. |
| **#6 Atlikti BDAR ir IT / IT saugos mokymus**  Mokymai yra vienas iš įrodymų parodantis, kad į reglamentą yra žiūrima rimtai. |
| **#7 Mobilių įrenginių centralizuotas valdymas**  Rekomenduojame įvertinti galimybes padidinti mobilių įrenginių saugumą, panaudojant mobilių įrenginių antivirusinę programinę įrangą, įrenginių šifravimą, galimybę distanciniu būdu padaryti viso turinio išmaniajame telefone ištrynimą, jei jis pamestas ar pavogtas (angl. „remote flush“) ar platesnes mobilių įrenginių valdymo galimybes. |
| **#8 Įdiegti automatizuotus asmens duomenų paieškos sprendimus IT sistemose**  Kritinėse sistemose (MS Dynamics Navision, Atsarginių kopijų sistemoje, Elektroninio pašto sistemoje, Failų serveryje, Avilda, CRM, Euroskaita ir ERP), kuriose saugomi didžiausi duomenų ir asmens duomenų kiekiai, esant galimybei (jei sistema leidžia tai padaryti) įdiegti sprendimus (sistemų patobulinimus), leidžiančius automatinėmis priemonėmis identifikuoti ir kategorizuoti asmens duomenis, o esant poreikiui ir juos ištrinti. |
| **#9 Nešiojamų laikmenų naudojimo tikslingumas bei alternatyvos**  Nešiojamos USB laikmenos gali būti panaudotos bet kurioje darbo vietoje, apribojimas netaikomas. Kadangi USB raktų naudojimo funkcionalumas ir tikslingumas yra abejotinas, mūsų nuomone geresnė alternatyva yra debesų kompiuterijos paslaugos, kuriose prieiga prie duomenų yra ribojama, duomenys. Alternatyva paprastam USB raktui galėtu būti šifruotas USB raktas. Tokio rakto naudojimas leistų užtikrinti, kad net ir pametus USB raktą su svarbia informacija, šių duomenų pašaliniai asmenys negalės panaudoti ir prievolės informuoti VDAI nelieka. Rekomenduojame keletą tokių turėti, jeigu toks poreikis keistis duomenimis atsirastų, taip pat rekomenduojame naudoti technines priemones, kurios blokuoja išorinių įrenginių naudojimą. Naudoti tik autorizuotus USB raktus. Naudojant USB, juos šifruoti. Drausti auto-run funkciją kompiuteriuose. |
| **#10 Užtikrinti tinkamą kompiuterinių darbo vietų apsaugą**   1. Vartotojų paskyrų slaptažodžius keisti ne rečiau kaip kas 60d.; 2. Apsirašyti ir pasitvirtinti slaptažodžių keitimo ir sudėtingumo politikas; 3. Apsirašyti ir pasitvirtinti naudojamų programų sąrašą; 4. Vartotojų naudojamuose įrenginiuose (kompiuteriuose, mobiliuosiuose įrenginiuose bei planšetėse) įdiegti licencijuotą (legalią) antivirusinio ir/ar kito kibernetinio saugumo sprendimą. 5. Įsitikinti, jog darbuotojai negalėtų naudoti administratoriaus teisių kompiuterinėse darbo vietose. Užtikrinti, jog administratoriaus slaptažodį žinotų tik už IT infrastruktūrą atsakingas asmuo arba 3 šalis, kuri teikia kompiuterinių darbo vietų priežiūros paslaugas. |
| **#15 Asmens duomenys IT sistemose**  Rekomenduojama atidžiai įvertinti,   1. ar ne per ilgai tvarkomi asmens duomenys IT sistemose ir nustatyti duomenų tvarkymo duomenų bazėse terminą; 2. ar IT sistemose netvarkomi pertekliniai duomenys. |

# 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/>