VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

FUNDAMENTINIŲ MOKSLŲ FAKULTETAS

INFORMACINIŲ TECHNOLOGIJŲ KATEDRA

Martynas Valauskis

BENDROJO DUOMENŲ APSAUGOS REGLAMENTO ĮGYVENDINIMO GEODEZINIŲ PASLAUGŲ ĮMONĖJE GALIMYBIŲ STUDIJA

A STUDY ON THE IMPLEMENTATION OF GENERAL DATA PROTECTION REGULATION IN THE SURVEYING COMPANY

Baigiamasis magistro darbas

Informacinių technologijų valdymo studijų programa, valstybinis kodas 621I13001

Informatikos studijų kryptis

Vilnius, 2019

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
FUNDAMENTINIŲ MOKSLŲ FAKULTETAS
INFORMACINIŲ TECHNOLOGIJŲ KATEDRA

TVIRTINU
Katedros vedėjas

(Parašas)

(Vardas, pavardė)

(Data)

Martynas Valauskis

BENDROJO DUOMENŲ APSAUGOS REGLAMENTO ĮGYVENDINIMO GEODEZINIŲ PASLAUGŲ ĮMONĖJE GALIMYBIŲ STUDIJA

A STUDY ON THE IMPLEMENTATION OF GENERAL DATA PROTECTION REGULATION IN THE SURVEYING COMPANY

Baigiamasis magistro darbas

Informacinių technologijų valdymo studijų programa, valstybinis kodas 621I13001

Informatikos studijų kryptis

Vadovas doc. dr. Irma Šileikienė (Pedag. vardas, vardas, pavardė) (Parašas) (Data)

Konsultantas dr. Aušra Žemienė (Pedag. vardas, vardas, pavardė) (Parašas) (Data)

Vilnius, 2019

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

FUNDAMENTINIŲ MOKSLŲ FAKULTETAS

INFORMACINIŲ TECHNOLOGIJŲ KATEDRA

TVIRTINU
Katedros vedėjas

(Parašas)

(Vardas, pavardė)

(Data)

BAIGIAMOJO MAGISTRO DARBO UŽDUOTIS

…….....Nr. .....

Vilnius

Studentui Martynui Valauskiui
(Vardas, pavardė)

Baigiamojo darbo tema: Bendrojo duomenų apsaugos reglamento įgyvendinimo geodezinių paslaugų įmonėje galimybių studija

patvirtinta 2019 m. kovo 06 d. dekano potvarkiu Nr. 147fm

Baigiamojo darbo užbaigimo terminas 2019 m. gegužės 23 d.

BAIGIAMOJO DARBO UŽDUOTIS:

Baigiamojo darbo tikslas yra įgyvendinti Bendrojo Duomenų Apsaugos Reglamento reikalavimus geodezinių paslaugų įmonėje, įvertinant išorines ir vidines grėsmes, siekiant užkirsti kelią galimam asmens duomenų nutekėjimui arba praradimui.

Baigiamojo bakalauro darbo konsultantai: dr. Aušra Žemienė
(Pedag. vardas, vardas, pavardė)

Vadovas _____ doc. dr. Irma Šileikienė
(Parašas) (Pedag. vardas, vardas, pavardė)

Užduotį gavau

(Parašas)

Martynas Valauskis
(Vardas, pavardė)

2017 m. lapkričio 16 d.
(Data)

Vilniaus Gedimino technikos universitetas
Fundamentinių mokslų fakultetas
Informacinių technologijų katedra

ISBN ISSN
Egz. sk. .....
Data .....-.....-.....

Antrosios pakopos studijų **Informacinių technologijų valdymo** programos magistro baigiamasis darbas
Pavadinimas **Bendrojo duomenų apsaugos reglamento įgyvendinimo geodezinių paslaugų įmonėje galimybių studija**
Autorius **Martynas Valauskis**
Vadovas **Irma Šileikienė**

Kalba: lietuvių

Anotacija

Baigiamajame magistro darbe nagrinėjami Europos Sąjungos Bendrojo duomenų apsaugos reglamento taikymo ypatumai, vertinamas jo reikalingumas geodezines paslaugas teikiančios įmonės veikloje. Išnagrinėti pagrindiniai asmens duomenų apsaugą Europos Sąjungoje reglamentuojantys teisės aktai. Įvertinti geodezinėje veikloje naudojami asmens duomenys, procesai, kuriuose jie naudojami, bei jiems kylančios grėsmės. Nustačius sritis, kuriose įmonės procesai neatitinka Bendrojo duomenų apsaugos reglamento reikalavimų, pateikiami technologiniai sprendimai jų stiprinimui. Baigiamajame darbe praktiškai ištestuoti populiariausi vaizdų redagavimo, duomenų šifravimo ir nuotolinio prisijungimo produktai. Išnagrinėjus teorinius asmens duomenų apsaugos ES aspektus ir praktinius duomenų apsaugos geodezine veikla užsiimančios įmonės veiklos ypatumus, pateikiamos baigiamojo magistro darbo išvados ir siūlymai.

Darbą sudaro 5 dalys: įvadas, asmens duomenų apsaugos strategija, asmens duomenų apsaugos užtikrinimas geodezinių paslaugų įmonėje, išvados ir rekomendacijos, literatūros sąrašas.

Darbo struktūra: Darbo apimtis – 61 p. teksto be priedų, 24 iliustr., 3 lent., 22 bibliografiniai šaltiniai.
Atskirai pridedami darbo priedai.

Prasminiai žodžiai: BDAR, asmens duomenys, 3D skenavimas, geodezinės paslaugos, vaizdų apdorojimas, šifravimas, nuotolinis prisijungimas.

Vilnius Gediminas Technical University
Faculty of Fundamental Sciences
Department of Information Technologies

ISBN ISSN
Copies No. .....
Date .....-.....-.....

Master Degree Studies **Information Technology Management** study programme Master Graduation Thesis

Title **A Study on the Implementation of General Data Protection Regulation in the Surveying Company**

Author **Martynas Valauskis**

Academic supervisor **Irma Šileikienė**

Thesis language: Lithuanian

Annotation

The Master's thesis examines specifics of the application of the European Union General Data Protection regulation and it's necessity in surveying company activity. The main legislation, regulating the protection of personal identifiable data in The European Union has also been analysed. The thesis is also assessing the personal data used in surveying company, business processes, in which they are used, and threats they are facing in it. Company's business processes are assessed against requirements of General Data Protection Regulation. Technical solutions are provided to strengthen business processes that does not meet criteria. Most popular image editing, data encryption and remote access software are tested in the thesis. The conclusions and suggestions of the final thesis is provided after theoretical aspects and the specifics of the surveying company's activity in data protection is analysed.

Structure: introduction, strategy of personal data protection, ensuring of personal data protection in surveying company, conclusions and recommendations, references.

Thesis consist of: 61 p. text without appendixes, 24 pictures, 3 tables, 22 bibliographical entries.
Appendixes included.

Keywords: GDPR, personal identifiable data, 3D scanning, surveyors services, image editing, data encryption, remote access.

Paveiksliukų sąrašas

2.1 pav. Trimatis vietovės vaizdas 23
2.2 pav. Panoraminis vietovės vaizdas [12] 24
2.3 pav. VĮ Registrų Centro išrašo pavyzdys 25
2.4 pav. Trimačio vaizdo ir nuotraukos palyginimas 29
2.5 pav. Photoshop pagrindinis redagavimo langas 31
2.6 pav. Photoshop CC įrašymo langas 32
2.7 pav. Nuotrauka prieš ir po redagavimo Photoshop programa 33
2.8 pav. Pagrindinis GIMP redagavimo langas 34
2.9 pav. GIMP failo eksportavimo langas 35
2.10 pav. PhotoScape X programos redagavimo langas 36
2.11 pav. Nuotraukos įrašymo langas 36
2.12 pav. Duomenų perkėlimo procesas 39
2.13 pav. Laiško naujam vykdytojui šablonas 40
2.14 pav. Teisės būti pamirštam procesas 42
2.15 pav. Duomenų sunaikinimo patvirtinimo laiško šablonas 43
2.16 pav. SensiGuard pagrindinis langas 44
2.17 pav. Pagrindinis Secure IT meniu langas 45
2.18 pav. Slaptažodžio su užuomina kūrimas 46
2.19 pav. Šifravimas išoriniams vartotojams 46
2.20 pav. Pagrindinis 7-Zip File Manager meniu langas 47
2.21 pav. Glaudinimo ir slaptažodžio pasirinkimo langas 48
2.22 pav. Standartinė ESET Secure Autentication veikimo schema [3] 51
2.23 pav. Prisijungimo patvirtinimas SecurAccess mobiliojoje programėlėje [20] 53
2.24 pav. Pranešimo apie duomenų apsaugos pažeidimą procesas 55

Lentelių sąrašas

2.1 lentelė. Sąnaudų palyginimas 30
2.2 lentelė. Vaizdų redagavimo programų palyginimas 37
2.3 lentelė. Šifravimo programų palyginimas 49

Santrumpų sąrašas

angl. – angliškai

AES – pažangus šifravimo standartas (angl. *Advanced Encryption Standard*)

BDAR – Bendrasis duomenų apsaugos reglamentas

EB – Europos Bendrija

EN – anglų kalba

ES – Europos Sąjunga

Eur – euras

HDD – standusis diskas (angl. *hard disk drive*)

IEC – tarptautinė elektrotechnikos bendrija (angl. *International Electrotechnical Commission*)

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

IT – informacinės technologijos

JAV – Jungtinės Amerikos Valstijos

LST – Lietuvos standartas

QR – QR kodas (angl. *quick response code*)

pav. - paveikslas

PRO – profesionalus

SMS – trumpoji žinutė (angl. *short message service*)

UAB – uždaroji akcinė bendrovė

USB – universalioji jungtis (angl. *Universal Serial Bus*)

VDAI – Valstybinė duomenų apsaugos inspekcija

VĮ – Valstybės įmonė

VM – virtualioji mašina (angl. *Virtual machine*)

VPN – virtualus privatus tinklas (angl. *virtual private network*)

3D – trijų dimensijų

Turinys

Įvadas 10

1. Asmens duomenų apsaugos strategija 12

1.1. Europos Sąjungos asmens duomenų apsaugos reglamentavimas 12

1.2. Standarto ISO/IEC 27040:15 Informacinės technologijos. Saugumo metodai. Saugojimo saugumas. Apžvalga. 18

1.3. Asmens duomenų apsaugos problemų sprendimai mokslinėje literatūroje 20

1.4. Apibendrinimas 22

2. Asmens duomenų apsaugos užtikrinimas geodezinių paslaugų įmonėje 23

2.1. Geodezinių paslaugų įmonės UAB „LiMAP“ esamos situacijos apžvalga 23

2.2. Duomenų subjekto informavimas apie duomenų rinkimą 26

2.3. Duomenų apsaugos pareigūno pareigybės įsteigimas 27

2.4. Asmens duomenų maskavimas tretiesiems asmenims siunčiamuose matavimo duomenyse 28

2.5. Perteklinės informacijos maskavimas nuotraukose 31

2.6. Duomenų perkeliamumo įgyvendinimas 38

2.7. Teisės būti pamirštam įgyvendinimas 41

2.8. Jautrios informacijos šifravimo ir negrįžtamo naikinimo programų palyginimas 43

2.9. Nuotolinio prisijungimo prie įmonės tinklo saugumo gerinimas 49

2.10. Pranešimas apie duomenų apsaugos pažeidimą 54

2.11. Apibendrinimas 56

Išvados 57

Rekomendacijos 57

Literatūros sąrašas 59

Priedai 61

A priedas. UAB „LiMAP“ pažyma. 62

B priedas. Matavimo darbų atlikimo sutarties pavyzdys. 64

Įvadas

Aktualumas. Asmens duomenų apsauga, tobulėjant informacinėms technologijoms, tampa vis didesniu iššūkiu išsivysčiusiose šalyse. Vis daugiau paslaugų yra perkeliama į internetą. Dabar jau ne tik nusipirkti norimą rūbą ar kitą prekę galima neišeinant iš namų. Didžioji dalis valstybinių įstaigų, finansų sektoriaus įmonių ir kitas paslaugas gyventojams bei verslui teikiančių įmonių savo paslaugomis skatina naudotis elektroninėje erdvėje. Tačiau tam, kad toks paslaugų lygis būtų užtikrintas, paslaugų tiekėjams reikalinga prieiga prie kliento asmens duomenų. Tokia informacija yra labai vertinga komercine ir rinkodaros prasme, todėl ja gali būti piktnaudžiaujama – tiek perduodant ar parduodant informaciją tretiesiems asmenims, tiek naudojant ją savo produkto reklamavimui jau esamiems klientams. Siekiant užtikrinti, kad tokia informacija būtų naudojama atsakingai ir nebūtų renkama bei tvarkoma perteklinė informacija, visoje Europos Sąjungoje nuo 2018 metų gegužės 25 dienos įsigaliojo Bendrasis duomenų apsaugos reglamentas (BDAR). Jis be išimčių privalomas visose valstybėse narėse, taigi, ir Lietuvoje. Visos įmonės, nepriklausomai nuo jų dydžio ir veiklos srities, privalo vadovautis Reglamento reikalavimais. Todėl prieš jam įsigaliojant, ar prieš įmonei pradedant teikti naujas paslaugas, turi būti pasiruošta Reglamento taikymui.

Darbo tikslas. Baigiamojo darbo tikslas yra įgyvendinti BDAR reikalavimus geodezines paslaugas teikiančioje įmonėje ir įvertinti išorines bei vidines grėsmes.

Baigiamojo darbo tikslui pasiekti iškelti tokie **uždaviniai:**

1. Išanalizuoti BDAR aktualumą šiuolaikinėje IT grįstoje darbo aplinkoje.
2. Įvertinti esamą duomenų apsaugos srities situaciją įmonėje.
3. Nustatyti BDAR reikalavimus, kurių taikymas privalomas įmonės veikloje.
4. Parengti veiksmų planą, užtikrinantį asmens duomenų apsaugą įmonėje.

Darbo praktinė vertė. Geodezines paslaugas teikiančioje įmonėje dabar yra naudojamos pažangios matavimų technologijos, leidžiančios vienu metu surinkti didelį kiekį informacijos, tarp kurių patenka ir kai kurie asmens duomenys. Tam, kad ši informacija būtų tinkamai naudojama ir saugoma, būtina užtikrinti, kad įmonėje naudojami procesai atitiktų griežtus Reglamento nuostatus. Šiame darbe yra pateikiami praktiniai ir techniniai pasiūlymai stiprinantys asmens duomenų apsaugą įmonės veiklos procesuose.

Taikyti metodai. Šiame darbe taikyti šie tyrimo metodai:

- **Mokslinės literatūros analizė.** Vertinta asmens duomenų samprata Europos Sąjungoje ir Jungtinėse Amerikos Valstijose, išskiriant pagrindinius panašumus ir skirtumus.
- **Dokumentų turinio analizė**. Išnagrinėti asmens duomenų apsaugą reglamentuojantys Europos Sąjungos teisės aktai bei su jais suderinti Lietuvos nacionalinės teisės aktai.
- **Veiklos analizė.** Įvertinta įmonės veikla ir joje naudojami asmens duomenys.
- **Testavimas.** Testuoti populiariausi duomenų apsaugą stiprinantys IT sprendimai.

Darbo aprobavimas. Darbas atliktas bendradarbiaujant su geodezinių paslaugų įmone UAB „LiMAP“. A priede pateikta UAB „LiMAP“ pažyma.

Darbą sudaro 5 dalys: įvadas, asmens duomenų apsaugos strategija, asmens duomenų apsaugos užtikrinimas geodezinių paslaugų įmonėje, išvados ir rekomendacijos, literatūros sąrašas.

Darbo struktūra: Darbo apimtis – 61 p. teksto be priedų, 24 iliustr., 3 lent., 22 bibliografiniai šaltiniai.

Atskirai pridedami darbo priedai.

1. Asmens duomenų apsaugos strategija

1.1. Europos Sąjungos asmens duomenų apsaugos reglamentavimas

1.1.1. Asmens duomenų apsaugos Europoje ištakos

Asmens duomenų apsauga Europos Sąjungoje (toliau – ES) yra viena iš pagrindinių asmens teisių išdėstytų Europos Sąjungos pagrindinių teisių chartijoje. Jos aštuntas straipsnis numato, kad: Kiekvienas turi teisę į savo asmens duomenų apsaugą [8] bei Tokie duomenys turi būti tinkamai tvarkomi ir naudojami tik konkretiems tikslams ir tik atitinkamam asmeniui sutikus ar kitais įstatymo nustatytais teisėtais pagrindais [8]. Pirmosios užuominos apie asmens duomenų apsaugą atsirado 1950 m. priimtoje Europos žmogaus teisių konvencijoje, kurioje buvo užtikrinta žmogaus teisė į tai „[...] kad būtų gerbiamas jo privatus ir šeimos gyvenimas [...]“ [2]. Nors asmens duomenys nebuvo išskirti atskiru punktu, juos galima laikyti žmogaus privataus gyvenimo apsaugos pradžia, o į jo sudėtį įeina ir asmeniniai duomenys.

Pirmas duomenų apsaugos srityje teisiškai privalomas tarptautinis dokumentas buvo 1981 m. Europos Tarybos 108-oji konvencija dėl asmenų apsaugos automatizuotai tvarkant asmens duomenis. Jos tikslas – užtikrinti, kad „tvarkant asmens duomenis automatizuotai [...], visų šalių teritorijose būtų gerbiamos kiekvieno asmens [...] teisės ir pagrindinės laisvės [...].“ [1]

Visi šie dokumentai turi juridinę galią visoje ES ir dabar, tiesa, su tam tikrais pakeitimais ir papildymais. Dėl to galima teigti, kad asmens duomenų apsauga visada buvo ir yra viena pagrindinių visos ES prioritetinių sričių.

1.1.2. Šiuo metu galiojantys Europos Sąjungos teisės aktai

ES teisėje galioja „trijų ramsčių“ sistema, todėl iki 2018 metų gegužės galiojo įvairūs visiems trims ramsčiams priklausantys teisės aktai. Pirmam ramsčiui priklauso šie norminiai dokumentai:

- Direktyva 95/46/EB dėl duomenų apsaugos, kurią dabar pakeitė Bendrasis duomenų apsaugos reglamentas;
- Direktyva 2002/58/EB dėl privatumo apsaugos elektroninių ryšių sektoriuje;
- Reglamentas (EB) Nr. 45/2001 dėl Bendrijos institucijų ir įstaigų tvarkomų asmens duomenų.

Trečiajam ramsčiui priklausė Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos. Šį sprendimą nuo 2018 metų gegužės pakeitė Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens

duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo.

Taigi šiuo metu asmens duomenų apsaugą ES reglamentuoja anksčiau minėta direktyva dėl privatumo apsaugos elektroninių ryšių sektoriuje, reglamentas dėl Bendrijos institucijų ir įstaigų tvarkomų asmens duomenų bei naujieji nuo 2018 metų gegužės įsigalioję Bendrasis duomenų apsaugos reglamentas (ES) 2016/679 ir direktyva (ES) 2016/680. Plačiau išanalizuoti dabar galiojantys teisės aktai.

Direktyva 2002/58/EB dėl privatumo apsaugos elektroninių ryšių sektoriuje. Šios direktyvos pagrindinis tikslas yra apsaugoti fizinių asmenų privatumą naudojantis ryšio priemonėmis, tokiomis kaip telefoniniai pokalbiai, trumpieji pranešimai, elektroninis paštas ir kt. Svarbiausios direktyvoje įtvirtintos nuostatos susijusios su asmens duomenų apsauga yra šios:

- Asmuo gali atsisakyti suteikti leidimą ryšio paslaugos tiekėjui naudoti jo asmeninius duomenis tiesioginės rinkodaros tikslais ar dalintis asmens duomenimis su trečiomis šalimis be asmens sutikimo;
- Net turint tokį sutikimą asmeniniai duomenys gali būti saugomi tik tiek laiko, kiek yra būtina suteikti pridėtinės vertės paslaugą;
- Asmeninai duomenys gali būti naudojami tik tiek, kiek tai reikalinga pateikti vartotojui sąskaitas už suteiktas paslaugas;
- Prie asmeninės informacijos taip pat priskiriamai buvimo vietai, kurią galima nustatyti pagal elektroninio ryšio priemones, išimtis gali būti taikoma tik tokiu atveju, jeigu tai yra reikalinga vykdant teisėsaugos funkcijas ar kai reikia nustatyti asmens buvimo vietą, kad jį lengviau būtų pasiekti priešgaisrinės gelbėjimo, greitosios pagalbos ar policijos tarnyboms. [4]

Ši direktyva buvo priimta 2002 metais, taigi kai kurie joje numatyti reikalavimai, sparčiai tobulėjant informacinėms technologijoms, tapo neaktualūs arba pasenę. Tuo tikslu ji buvo dalinai koreguota 2009 metais, priimant Lisabonos sutartį (nauja ES sutartis pasirašyta 2009 metais). Šiuo metu ji vis dar galiojanti, bet praėjus beveik dešimtmečiui nuo paskutinių pakeitimų, vėl yra ruošiamas direktyvos pakeitimų projektas.

Reglamentas (EB) Nr. 45/2001 dėl Bendrijos institucijų ir įstaigų tvarkomų asmens duomenų. Šis reglamentas, įsigaliojęs 2001 metais, yra skirtas nustatyti, kaip turi būti ginamos fizinių asmenų teisės, tame tarpe, ir asmens duomenys Bendrijos institucijose. Šio reglamento vienas iš

pagrindinių punktų yra toks, kad institucijos gali rinkti tik tokius duomenis, kurie yra reikalingi tam tikroms funkcijoms atlikti, ir saugomi tol, kol jie yra aktualūs. Tokie duomenys negali būti naudojami jokiu kitu tikslu, nebent suinteresuotas asmuo sutiktų su tolesniu jo asmens duomenų tvarkymu. Tiesa, yra nustatyti tam tikri asmens duomenys, kurių negalima tvarkyti ir netgi prašyti asmens juos pateikti. Tai duomenys „[...] kurie atskleidžia asmens rasinę ir etninę kilmę, politinius filosofinius įsitikinimus, narystę profesinėse sąjungose ir duomenis apie sveikatą bei lytinį gyvenimą.“ [6] Šių duomenų tvarkymas daugeliu atveju draudžiamas net su aiškiu asmens sutikimu, leidžiančiu apdoroti tokius duomenis. Kaip ir anksčiau minėtoje direktyvoje, išimtis asmens duomenų tvarkymui yra taikoma tik tuo atveju, kai tai reikalinga nacionaliniam saugumui, visuomenės gerovei ar sklandžiam teisėsaugos darbui užtikrinti.

Šis reglamentas įveda vieną naują instituciją ES. Taip pat kiekvienoje Bendrijos institucijoje naują pareigybę. Kiekviena Bendrijos institucija privalo paskirti bent vieną asmenį savo viduje, kuris eitų duomenų apsaugos pareigūno pareigas. Jo pareigos yra:

- Užtikrinti, kad duomenų valdytojai ir duomenų subjektai būtų informuoti apie šiame reglamente nustatytas savo teises ir pareigas;
- Bendradarbiauti su Europos duomenų apsaugos priežiūros pareigūnu tiek, kiek tai liečia jo atstovaujamą instituciją;
- Užtikrinti, kad jo organizacijoje būtų laikomasi šio reglamento;
- Priimti pranešimus iš įstaigos darbuotojų apie galimus pažeidimus asmens duomenų srityje. [6]

Kita nauja institucija, viena visai ES, yra nepriklausoma priežiūros institucija: Europos duomenų apsaugos priežiūros pareigūnas. Šis pareigūnas paskiriamas bendromis Europos Parlamento ir Europos Tarybos pastangomis pagal Komisijos parengtą sąrašą. Europos duomenų apsaugos priežiūros pareigūnas atsako už tai, kad būtų užtikrinta, jog Bendrijos institucijos ir įstaigos, tvarkydamos asmens duomenis, gerbia fizinių asmenų pagrindines teises ir laisves, svarbiausia – jų teisę į privataus gyvenimo neliečiamumą“ [6].

Šis reglamentas vis dar galioja, tačiau, kaip ir anksčiau aprašyta direktyva, yra pateiktas jo pakeitimo projektas, kuris turėtų būti priimtas netolimoje ateityje.

Direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo. Šioje direktyvoje nustatytos taisyklės, susijusios su fizinių asmenų duomenų apsauga teisėsaugos institucijoms vykdant ikiteisminius tyrimus, bei kitus su nusikaltimais susijusius tyrimus. Taip pat nustatytos taisyklės duomenų naudojimui „[...]apsaugos nuo grėsmių visuomenės saugumui ir jų prevencijos tikslais“ [5].

Šioje direktyvoje be kita ko užtikrinama, kad draudimas dalintis asmens duomenimis su kitomis šalimis nebūtų kliūtis keistis duomenimis tarp skirtingų šalių institucijų, kai to reikalaujama pagal vienos iš šalių teisę.

Šia direktyva tvarkomi duomenys yra skirstomi į šiuos:

- duomenys asmenų, kurie galimai įvykdė arba rengiasi įvykdyti nusikalstamą veiką;
- duomenys asmenų, nuteistų už nusikalstamą veiką;
- duomenys asmenų, kurie buvo nusikalstamos veikos aukomis arba kurių atžvilgiu gali būti įvykdyti nusikaltimai;
- duomenys asmenų, kurie gali būti apklausiami atliekant tyrimus dėl nusikaltimų, kitaip tariant, liudininkai bei kiti suinteresuoti asmenys. [5]

Kaip ir reglamente Bendrijos institucijoms, taip ir šioje direktyvoje, yra apibrėžiama duomenų apsaugos pareigūno institucija. Kiekviena valstybės narės institucija turi paskirti pareigūną atsakingą už tai, kad jo atstovaujamoje valstybės institucijoje būtų laikomasi šios direktyvos nuostatų. Skirtingai nei Bendrijų institucijų atveju, šis pareigūnas gali būti paskiriamas atstovauti kelioms susijusioms institucijoms vienu metu.

Europos Parlamento ir Tarybos Reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. Toliau – Reglamentas. Šis reglamentas pakeitė anksčiau galiojusią direktyvą 95/46/EB. Dauguma šioje direktyvoje buvusių punktų, kurie vis dar yra aktualūs, buvo perkelta į naująjį reglamentą. Jo, kaip ir ankstesnės direktyvos, tikslas yra nustatyti taisykles, susijusias su fizinio asmens duomenų apsauga, ir tokių duomenų laisvu judėjimu ES viduje.

Pagrindiniai reglamente nustatyti asmens duomenų tvarkymo principai yra tokie, kad duomenys turi būti:

- tvarkomi teisėtų, sąžiningu ir skaidriu būdu;

- renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau nenaudojami jokiais kitais tikslais;
- adekvatūs, tinkami ir tik tokie, kokių reikia siekiant tikslų, dėl kurių jie buvo surinkti;
- tikslūs ir prireikus atnaujinami;
- laikomi tokia forma, kad asmens tapatybę būtų įmanoma nustatyti ne ilgiau, nei to reikia tais tikslais, kuriais asmens duomenys tvarkomi;
- tvarkomi taip, kad, taikant atitinkamas technines priemones, būtų užtikrinamas tinkamas duomenų saugumas. [7]

Šiuo reglamentu labiau akcentuojamas asmens sutikimas su jo duomenų tvarkymu. Prieš rinkdami bet kokius duomenis, įmonė ar organizacija turi tiksliai parašyti, kokiu tikslu ir kiek laiko bus saugomi asmens duomenys. Asmuo turi patvirtinti savo sutikimą, pavyzdžiui, padėdamas varnelę internetiniame puslapyje. Skirtumas nuo senosios tvarkos yra toks, kad formos negali būti paruoštos su iš anksto sudėtomis varnelėmis. Taip pat sąlygose negali būti punkto, „[...] kad turi būti duotas sutikimas tvarkyti asmens duomenis, kurie nėra būtini tai sutarčiai vykdyti.“ [7]

Asmuo turi teisę bet kada gauti informaciją iš bet kurios institucijos ar organizacijos apie tai, ar jo duomenys yra tvarkomi ir kokiu tikslu. Taip pat jis turi būti informuotas, jeigu jo duomenys perduodami trečiosioms šalims.

Dar viena naujovė reglamente yra asmeniui suteikiama teisė reikalauti, kad jo duomenys būtų ištrinti, dar vadinama teise būti pamirštam. Asmuo gali bet kuriuo metu reikalauti, kad duomenų valdytojas ištrintų visą apie jį sukauptą informaciją, jei asmens duomenys buvo tvarkomi neteisėtai, jie nebėra reikalingi tikslui, kuriuo jie buvo renkami, pasiekti, arba asmuo atšaukia savo duotą sutikimą tvarkyti jo duomenis.

Kiekviena įmonė ar organizacija nuo šiol privalės turėti aiškiai išdėstytas vidaus taisykles, susijusias su asmens duomenų apsauga. Su šiomis taisyklėmis turės susipažinti ir jų laikytis kiekvienas įmonės darbuotojas ar organizacijos narys.

Kaip ir anksčiau aprašytų direktyvų ir reglamentų atveju, šiame reglamente taip pat įvedama duomenų apsaugos pareigybė. Tik šiuo atveju tokia pareigybė bus privaloma visose valstybės įstaigose, bei įmonėse, užsiimančiose asmens duomenų tvarkymu automatizuotu būdu. Duomenų apsaugos pareigūno užduotys panašios kaip ir prieš tai aptartuose teisės aktuose:

- supažindinti organizacijos ar įmonės darbuotojus su šio reglamento reikalavimais ir užtikrinti, kad jų būtų laikomasi;

- konsultuoti dėl galimo poveikio duomenų apsaugai vertinimo;
- bendradarbiauti su priežiūros institucija. [7]

Šiame reglamente, skirtingai nei ankstesnėje direktyvoje, pažeidus asmens duomenų apsaugos taisykles, yra numatytos didelės baudos, galinčios siekti iki 20 mln. eurų.

Visi šie teisės aktai yra labai glaudžiai susiję ir kartu pabrėžia asmens duomenų apsaugos svarbą visos Sąjungos mastu. Jie yra priimti tam, kad būtų galima nustatyti bendras visai ES taisykles, o tai palengvina tiek institucijų bei organizacijų, kurios tvarko duomenis, tiek priežiūros institucijų darbą. Išanalizavus visus šiuos dokumentus, galima įvardinti pagrindines ES gaires asmens duomenų apsaugos srityje:

- Duomenys turi būti renkami tik turint teisėtą tikslą ir tik tokie, kurie yra reikalingi tam tikram tikslui pasiekti;
- Duomenys turi būti apsaugoti nuo galimo duomenų atskleidimo pašaliniams asmenims;
- Pasibaigus duomenų aktualumui, duomenys negali būti naudojami kitais tikslais;
- Elektroninėje erdvėje renkant duomenis, turi būti gautas aiškus asmens sutikimas tokių duomenų tvarkymui;
- Išimtis visoms šioms taisyklėms taikomos, kai duomenys tvarkomi siekiant užtikrinti nacionalinį saugumą, visuomenės gerovę bei teisėtvarkos institucijų sklandų darbą.

1.1.3. Europos Parlamento vaidmuo asmens duomenų apsaugos srityje

Europos Parlamentas visada pabrėžė būtinybę užtikrinti didesnio saugumo ir asmens privatumo bei asmens duomenų apsaugos pusiausvyrą. Parlamentas yra priėmęs įvairių rezoliucijų šiais opiais klausimais, ypatingą dėmesį skirdamas etninio ir rasinio profiliavimo, tarpvalstybinio bendradarbiavimo kovos su terorizmu ir tarpvalstybiniu nusikalstamumu srityje, kūno skenerių naudojimo siekiant stiprinti aviacijos saugumą, biometrinių duomenų naudojimo pasuose ir bendrų konsulinių instrukcijų, sienų valdymo, interneto ir duomenų gavybos klausimams.

1.1.4. Asmens duomenų apsaugos reglamentavimas Lietuvos teisėje

Lietuvoje asmens duomenų apsaugą prižiūri Valstybinė duomenų apsaugos inspekcija. Ji atlieka ir konsultuojančios, ir prižiūrinčios institucijos funkcijas. Inspekcija taip pat atsakinga už nuobaudų skyrimą organizacijoms, nesilaikančioms reglamento reikalavimų.

Lietuvai esant ES nare, visos anksčiau išvardintos Direktyvos ir Reglamentai yra taikomi tiesiogiai. Pagrindinis šiuo metu galiojantis įstatymas yra Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, priimtas dar 1996 m. Nors iki 2018 metų gegužės 6 dienos turėjo būti priimti visi privalomi įstatymo pakeitimai tam, kad būtų pasiruošta BDAR įsigaliojimui, nauja pagrindinio asmens duomenų apsaugą reglamentuojančio įstatymo redakcija buvo priimta tik 2018 metų birželio 30 d. Todėl, įsigaliojant Reglamentui, Lietuva kartu su dar septyniomis ES šalimis buvo įvardyta kaip šalis, laiku nepasiruošusi naujojo reglamento įgyvendinimui.

Šis įstatymas nustato Reglamento reikalavimų praktinį įgyvendinimą šalies mastu:

- Priežiūros institucijos steigimo tvarką, vadovų bei narių skyrimo tvarką;
- Patikrinimų bei audito vykdymą;
- Skundų pateikimo ir nagrinėjimo tvarką;
- Sankcijų skyrimo tvarką. [11]

1.2. Standarto ISO/IEC 27040:15 Informacinės technologijos. Saugumo metodai. Saugojimo saugumas. Apžvalga.

Pastarąjį dešimtmetį informacinėms technologijoms tobulėjant didžiuliu greičiu, vis didesnis dėmesys yra skiriamas informacinių technologijų saugumui. Tuo tikslu yra kuriamos galingos antivirusinės programos, diegiamos ugniasienės, trukdančios kenksmingoms programoms patekti į organizacijos internetinį tinklą. Tačiau ilgą laiką duomenų laikmenų apsaugai nebuvo skiriama reikiamo dėmesio dėl to, kad duomenų saugojimas buvo suprantamas kaip fizinis saugojimas kietajame diske ar serveryje, saugiai užrakintame kambaryje. Tačiau keičiantis technologijoms ir didėjant saugomų duomenų kiekiams, atsirado didžiulių duomenų centrų poreikis, debesų kompiuterijos saugyklos. Susidarė prielaidos didelei saugumo spragai atsirasti, nes reikėjo užtikrinti, kad duomenys būtų apsaugoti tiek juos perkeliant į nuotolines saugyklas, tiek saugant jose.

Problema tampa dar didesnė, kai kalbama apie jautrius duomenis, pavyzdžiui, organizacijos komercines paslaptis, finansinius, klientų bei darbuotojų duomenis ir informacija apie privačius asmenis. Tokių duomenų nutekėjimas organizacijai užtraukia įvairias neigiamas pasekmes: organizacijos komercinės paslaptys ir finansiniai rodikliai tampa žinomi konkurentams, sugadinama organizacijos reputacija. Šios pasekmės gali skaudžiai atsiliepti organizacijos finansiniam stabilumui ir ateities perspektyvoms. Tačiau skaudžiausiai finansiškai organizacija nukentėtų nutekėjus pagal įstatymą saugomiems duomenims, kurių pažeidimas užtrauktų organizacijai milijonines baudas.

Šis standartas buvo sukurtas kaip instrukcijos, kuriomis vadovaujantis, būtų suvienodinta duomenų saugojimo apsauga įvairiose organizacijose ir išvengta duomenų praradimų dėl sistemų

gedimų arba įsilaužimų. Taip pat jame atkreipiamas dėmesys į pagrindines grėsmes duomenų saugojimo saugumui. Šis standartas taikomas įvairiose organizacijose: privačiose įmonėse, valstybinėse įstaigose bei valstybės valdomose įmonėse, taip pat visose kitose organizacijose, kurios kaupia ar renka bet kokią informaciją. Tai ypač aktualu organizacijoms, renkančioms asmeninius duomenis apie gyventojus.

Remiantis Saugyklų saugumo standartu, galima teigti, kad pagrindinės grėsmės saugykloms yra:

- **Duomenų nutekėjimas.** Jis dažniausiai kyla dėl kenkėjiškų trečiųjų asmenų veiksmų arba dėl neatsakingo požiūrio į duomenų apsaugą. Didžiausią žalą organizacijai daro komercinių paslapčių, intelektinės nuosavybės, finansinių rodiklių bei privačių asmeninių duomenų nutekėjimas. Tai gali užtraukti didžiules baudas už įstatymo reikalavimų nevykdymą, sugadintą reputaciją ir prarastą klientų pasitikėjimą;
- **Duomenų sugadinimas arba sunaikinimas.** Ši grėsmė kyla dėl nepakankamo duomenų apsaugos lygio. Duomenis sugadinti gali pašalinio asmens neteisėtas prisijungimas prie sistemos. Tokiu atveju duomenys gali būti pakeisti, tai yra – nelieka duomenų vientisumo, arba sunaikinami, tai yra – panaikinama duomenų prieinamumo sąlyga. Gaisras, potvynis ar kiti naikinantys gamtos reiškiniai taip pat gali sunaikinti duomenis negrįžtamai. Tam gali pakakti ir dėl trumpo elektros jungimo laikinai išsijungusio duomenų serverio;
- **Laikinas arba nuolatinis prieigos netekimas;**
- **Įstatymo nustatytų reikalavimų nevykdymas.** Tai gali būti įvairūs duomenų apsaugos pažeidimai, susiję su skirtingais reikalavimais skirtingose šalyse, kai organizacija yra tarptautinė. Tačiau ir veikiant vienoje šalyje gali būti pažeidžiami reikalavimai, kaip duomenys turi būti renkami ir kiek laiko saugomi. [12]

Šioms grėsmėms valdyti yra rekomenduojama naudoti nuodugniąją apsaugą. Planuodama saugyklos apsaugą, įmonė turi įvertinti visų lygių ir įrenginių apsaugą: tinklų, įrenginių, aplikacijų ir sistemų. Tokiu būdu pasiekiama, kad įveikus vieną apsaugos lygį, kiti sistemos komponentai liktų apsaugoti, o visa sistema veikianti. Kokią apsaugą kiekvienam iš lygių pasirinkti lemia tai, koks yra saugomos informacijos jautrumas, įmonės veiklos pobūdis ir galinčios kilti grėsmės. Pagrindinės gairės yra šios:

- Apsauga turėtų būti fokusuota į tris pagrindines grupes: žmones, technologijas ir operacijas;

- Palaikyti matomą ir nuolat atnaujinamą sistemų apsaugos strategiją;
- Įdiegti apsaugos mechanizmus keliose sistemos dalyse, kad būtų apsiginta nuo visų galimų grėsmių ir atakų;
- Naudoti saugumo spragų aptikimo mechanizmus;
- Nuolat vykdyti saugumo bandymo testus;
- Sekti ir analizuoti šiuo metu vyraujančias grėsmes. [12]

1.3. Asmens duomenų apsaugos problemų sprendimai mokslinėje literatūroje

Viena iš problemų, kylančių kalbant apie asmens duomenis, yra vadinamųjų didžiųjų duomenų (*angl. big data*) naudojimas. Didieji duomenys įvairioje mokslinėje literatūroje apibūdinami skirtingai. „Didieji duomenys gali būti suprantami kaip galingesnis duomenų paieškos būdas, kuris priklauso nuo didelių duomenų kiekių, greitesnių kompiuterių ir naujų analitinių technikų, kuris įgalina išgauti reikiamą informaciją“ (Rubinstein, 2013) [16]. Bendra prasme didieji duomenys yra didelės duomenų bazės su asmenine informacija, pavyzdžiui, šeimos nariai, darbovietė, internetinio apsipirkimo istorija ir interneto naršymo istorija. Visi šie duomenys saugomi bendrose duomenų bazėse, todėl verslui yra neįkainojama informacija, siekiant kuo daugiau sužinoti apie potencialius savo klientus, ir pasiūlyti jiems tai, ko reikia. Tačiau tai taip pat sukelia ir didelių problemų duomenų apsaugos srityje. Pirmiausia todėl, kad asmeninė informacija yra skirtingai traktuojama įvairiose pasaulio šalyse.

Europos Sąjunga šiuo metu plačiausiai apibūdina asmeninę informaciją. Jai priskiriama žmogaus amžius, uždarbis, kredito reitingas, duomenys apie nuosavybę, fizinę būklę, šeimyninę padėtį, hobius ir internetinio naršymo bei pirkimo istorija. Šis sąrašas nėra baigtinis. Tuo tarpu Jungtinėse Amerikos Valstijose (toliau – JAV) bei Japonijoje šis sąrašas daug trumpesnis. Jį sudaro tik amžius, gyvenamoji vieta, turima nuosavybė ir internetinio naršymo bei pirkimo istorija [21]. Todėl asmens duomenų apsaugą suderinti yra sunku. Tai taip pat apsunkina keitimąsi asmens duomenimis tarp šių šalių.

Pagrindiniai skirtumai tarp JAV ir ES (Solove and Schwartz, 2013) yra šie:

- Europos Sąjungoje asmenine informacija laikoma visa informacija, kuria galima tiesiogiai arba netiesiogiai susieti su konkrečiu asmeniu. Taigi asmenine informacija laikoma netgi automatinė vietos nustatymo informacija ir internetinis vartotojo adresas, nes juos, įdėjus daugiau pastangų, galima susieti su konkrečiu asmeniu.

- Jungtinėse Valstijose pagrindinė problema yra tai, kad nėra vieno bendro apibrėžimo, kas yra asmeninė informacija. JAV teisėje kartu su terminu „asmeninė informacija“ yra naudojama ir „identifikuojanti informacija“. Dar daugiau sumaišties įneša tai, kad Jungtinėse Valstijose yra trys asmeninės informacijos traktavimai:
    - **Tautologinis.** Šis traktavimas labai populiarus visoje JAV teisėje, kurio pavyzdys gali būti greičio apribojimas „važiuoti priimtinu greičiu“ arba „klausyti tinkamo asmens nurodymų“, kurie nieko iš esmės nenurodo. Šiuo atveju, asmenį identifikuojanti informacija yra laikoma tokia informacija, kuri identifikuoja asmenį.
    - **Nevieša informacija.** Šis traktavimas asmenine informacija laiko tokią informaciją, kuri negali būti pasiekiama viešai. Čia atsiranda prieštaravimas, kai, pavyzdžiui, vardas, pavardė ir adresas yra laikoma vieša informacija, nes ji gali būti randama telefonų knygoje, bet dauguma žmonių šiuos duomenis laiko savo pačia svarbiausia asmenine informacija.
    - **Specifinė informacija.** Šis traktavimas nustato sąrašą, kokia informacija gali būti laikoma asmenine, pavyzdžiui vardas kartu su bet kuria kita viena informacijos rūšimi, tokia kaip socialinio draudimo numeris, vairuotojo pažymėjimo numeris ar banko sąskaitos numeris. Šis traktavimas neįtraukia daugumos informacijos rūšių, kurios vienos arba su vardu, lengvai identifikuoja asmenį. [19]

Kad supaprastinti keitimąsi duomenimis autoriai, siūlo įvesti tris asmeninės informacijos kategorijas:

- **Nustatanti informacija (angl. *identified*).** Šiai informacijai priklauso tokie duomenys, kuriais tiesiogiai galima atskirti konkretų asmenį. Tokiai informacijai būtų priskiriama visa jautri informacija, įskaitant informaciją apie asmens rasinę ir etninę kilmę, religinius, politinius įsitikinimus ir sveikatą. Tokiai informacijai būtų taikomas aukščiausias apsaugos lygis.
- **Galimai nustatanti informacija (angl. *identifiable*).** Tokiai informacijai priskiriami duomenys, kurie tiesiogiai neidentifikuoja asmens, tačiau yra nedidelė tikimybė, kad ateityje ši informacija gali būti tam tikrose situacijose susieta su konkrečiu asmeniu. Tokios informacijos tvarkymas turėtų būti reguliuojamas, bet ne taip griežtai, kaip pirmos kategorijos duomenys.

- Žemiausiai apsaugos kategorijai būtų priskirta **neidentifikuojanti informacija**, kuri, nors ir gali turėti asmeninių duomenų požymių, tačiau yra praktiškai ir protingomis priemonėmis nesusiejama su atskiru asmeniu. Tokiai informacijai dažniausiai galima būtų priskirti tam tikrus statistinius duomenis. [19]

JAV teisėje šias kategorijas būtų galima įgyvendinti gana lengvai, nes nėra vieningo asmens duomenų apibrėžimo, o jų apsauga nėra aiškiai apibrėžta. Tačiau sunkiau būtų jas suderinti su ES teise. Ypač žinant, kad su naujuoju duomenų apsaugos reglamentu yra dar labiau griežtinamos duomenų apsaugos taisyklės. Tiesa, šios kategorijos galėtų būti gera pradžia siekiant sukurti kuo glaudesnį duomenų keitimosi reguliavimą tarp Jungtinių Valstijų ir Europos Sąjungos.

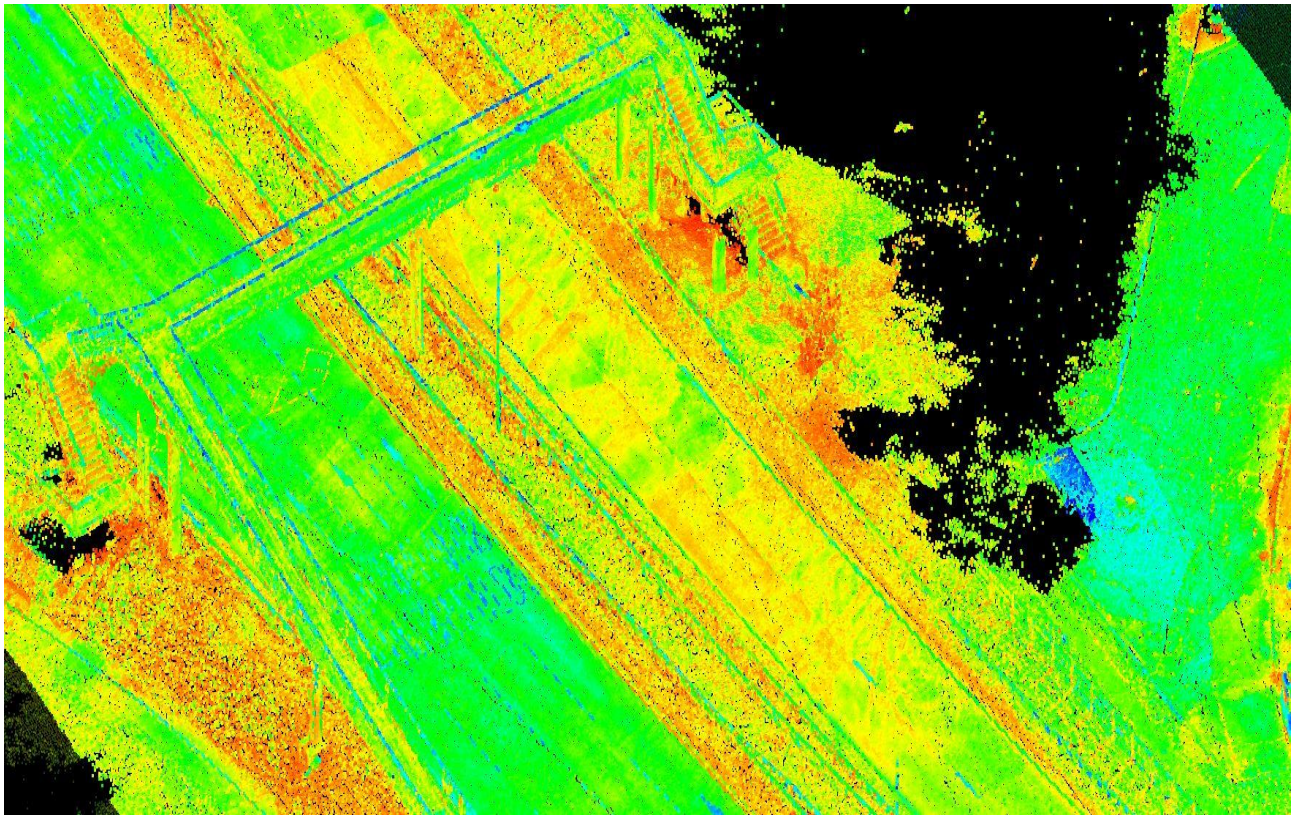
1.4. Apibendrinimas

Šiame skyriuje išanalizuoti asmens duomenų apsaugą ES reglamentuojantys teisės aktai bei jų taikymo sritys. Pagrindinis šios srities norminis aktas, privalomas visoms valstybėms narėms, yra Bendrasis duomenų apsaugos reglamentas, kurio svarbiausios nuostatos, užtikrinančios tinkamą kiekvieno asmens duomenų apsaugą, yra teisė nesutikti su duomenų tvarkymu, teisė būti tinkamai informuotam apie jo duomenų rinkimą ir rinkimo tikslus, bei draudimas rinkti ir tvarkyti asmens duomenis, kurie nėra reikalingi tam tikslui pasiekti. Šis Reglamentas galioja visoms įmonėms, organizacijoms vykdančioms veiklą Bendrijos teritorijoje bei valstybinėms įstaigoms.

2. Asmens duomenų apsaugos užtikrinimas geodezinių paslaugų įmonėje

2.1. Geodezinių paslaugų įmonės UAB „LiMAP“ esamos situacijos apžvalga

UAB „LiMAP“ yra įsikūrusi Saulėtekio Slėnio mokslo ir technologijų parke. Pagrindinė įmonės veikla yra geodeziniai matavimai. Įmonėje vidutiniškai dirba 10 darbuotojų. Matavimams naudojama moderni mobili 3D skenavimo įranga, sumontuota ant automobilio. Ši įranga surenka ir ekrane pateikia trimatį vietovės vaizdą (2.1 pav.).



2.1 pav. *Trimatis vietovės vaizdas*

Tuo pat metu daromos panoraminės nuotraukos, kurios padeda braižytojui lengviau atpažinti vietovėje esančius objektus (2.2 pav.). Surinkti matavimų duomenys yra apdorojami įmonės darbuotojų ir perduodami braižytojui. Tai gali būti įmonės darbuotojas arba subrangovas kitoje Europos Sąjungos arba trečiojoje šalyje.

2.1.2. Įmonės renkami asmens duomenys

Skenuojant ir fotografuojant vietovę yra surenkami erdviniai duomenys apie esamą vietovės vaizdą. Tačiau neišvengiamai yra užfiksuojami ir duomenys, kurie gali būti laikomi asmens duomenimis, tai yra:

- žmonių veidai;
- automobilių registracijos numeriai;
- pastatų adresai.

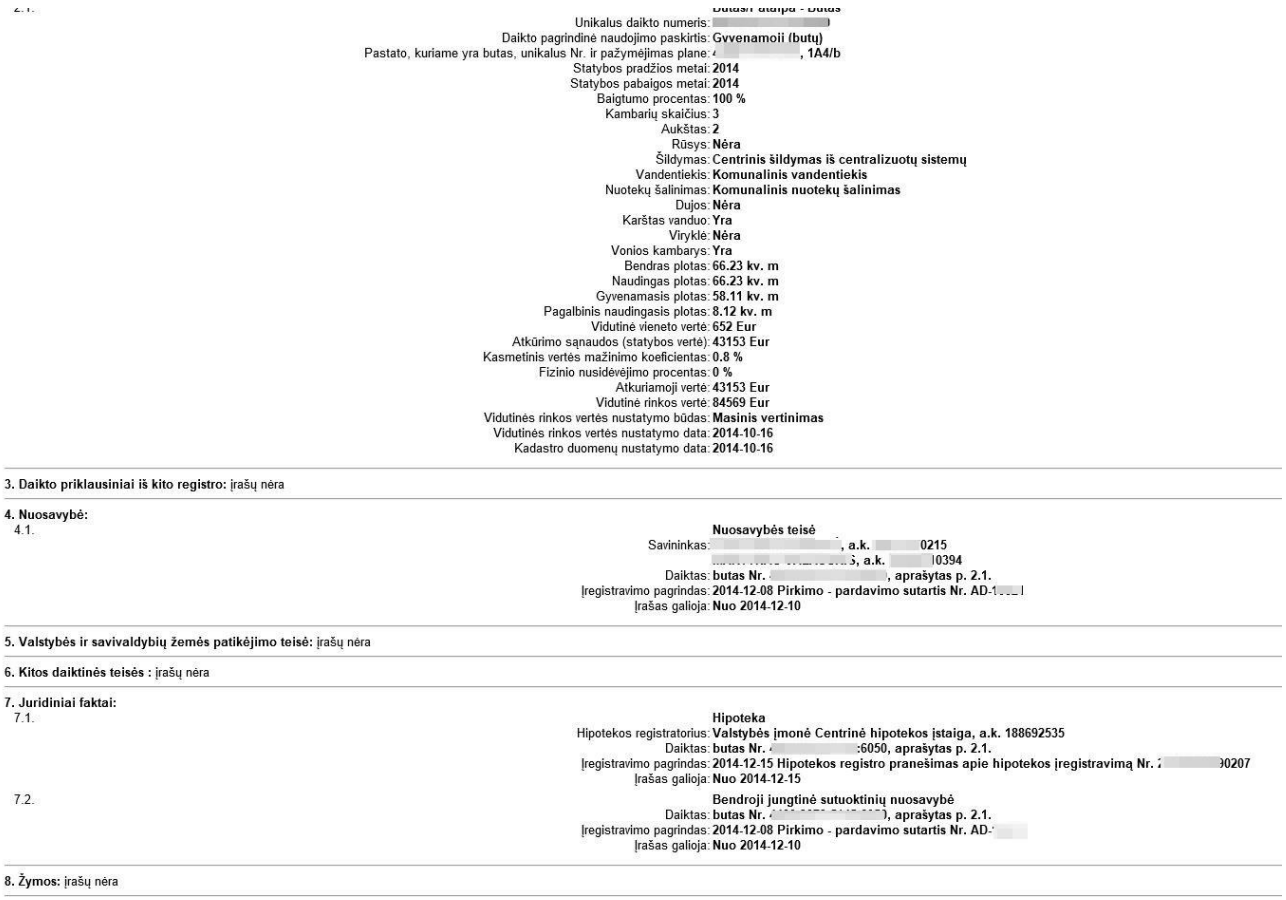


2.2 pav. *Panoraminis vietovės vaizdas [12]*

Ši informacija nėra reikalinga darbui atlikti, todėl pagal Bendrojo duomenų apsaugos reglamento 5 straipsnį, yra laikoma pertekline informacija.

Atliekant matavimus, iš Registrų centro yra gaunami matuojamų sklypų ir pastatų nuosavybės teisę patvirtinantys dokumentai. Šiuose dokumentuose nurodomi savininkų asmeniniai duomenys:

vardas, pavardė, amžius bei adresas ir turimi įsipareigojimai bankams. Taip pat, esant keliems savininkams, galima matyti jų giminystės ryšius (2.3 pav.).


Unikalus daikto numeris:
Daikto pagrindinė naudojimo paskirtis: Gyvenamoii (butų)
Pastato, kuriame yra butas, unikalus Nr. ir pažymėjimas plane: , 1A4/b
Statybos pradžios metai: 2014
Statybos pabaigos metai: 2014
Baigtumo procentas: 100 %
Kambarių skaičius: 3
Aukštas: 2
Rūsys: Nėra
Šildymas: Centrinis šildymas iš centralizuotų sistemų
Vandentiekis: Komunalinis vandentiekis
Nuotekų šalinimas: Komunalinis nuotekų šalinimas
Dujos: Nėra
Karštas vanduo: Yra
Viryklė: Nėra
Vonios kambarys: Yra
Bendras plotas: 66.23 kv. m
Naudingas plotas: 66.23 kv. m
Gyvenamasis plotas: 58.11 kv. m
Pagalbinis naudingasis plotas: 8.12 kv. m
Vidutinė vieneto vertė: 652 Eur
Atkūrimo sąnaudos (statybos vertė): 43153 Eur
Kasmetinis vertės mažinimo koeficientas: 0.8 %
Fizinio nusidėvėjimo procentas: 0 %
Atkuriamoji vertė: 43153 Eur
Vidutinė rinkos vertė: 84569 Eur
Vidutinės rinkos vertės nustatymo būdas: Masinis vertinimas
Vidutinės rinkos vertės nustatymo data: 2014-10-16
Kadastro duomenų nustatymo data: 2014-10-16

3. Daikto priklausiniai iš kito registro: įrašų nėra

4. Nuosavybė:
4.1. Nuosavybės teisė
Savininkas: , a.k. 0215
, a.k. 0394
Daiktas: butas Nr. , aprašytas p. 2.1.
Įregistravimo pagrindas: 2014-12-08 Pirkimo - pardavimo sutartis Nr. AD-1
Įrašas galioja: Nuo 2014-12-10

5. Valstybės ir savivaldybių žemės patikėjimo teisė: įrašų nėra

6. Kitos daiktinės teisės : įrašų nėra

7. Juridiniai faktai:
7.1. Hipoteka
Hipotekos registratorius: Valstybės įmonė Centrinė hipotekos įstaiga, a.k. 188692535
Daiktas: butas Nr. :6050, aprašytas p. 2.1.
Įregistravimo pagrindas: 2014-12-15 Hipotekos registro pranešimas apie hipotekos įregistravimą Nr. 0207
Įrašas galioja: Nuo 2014-12-15
7.2. Bendroji jungtinė sutuoktinių nuosavybė
Daiktas: butas Nr. , aprašytas p. 2.1.
Įregistravimo pagrindas: 2014-12-08 Pirkimo - pardavimo sutartis Nr. AD-
Įrašas galioja: Nuo 2014-12-10

8. Žymos: įrašų nėra

2.3 pav. *VĮ Registrų Centro išrašo pavyzdys*

Visi šie duomenys yra svarbūs rengiant matavimų dokumentaciją ir registruojant nekilnojamąjį turtą, bet yra labai jautrūs ir turi būti ypač saugomi nuo atskleidimo tretiesiems asmenims ar duomenų vagystės. Dokumentus iš registrų centro gali užsakyti ir gauti tik pats savininkas ir pats perduoti matavimus atliekančiai įmonei, popieriniu ar skaitmeniniu pavidalu.

Visi duomenys, išskyrus fotografijose užfiksuotus vaizdus, yra naudojami tik įmonės darbuotojų. Skenavimų metu užfiksuotos panoraminės nuotraukos dažniausiai siunčiamos anksčiau minėtiems subrangovams.

2.1.3. Įmonės informacinių technologijų apžvalga

Visi įmonės duomenys yra saugomi vietiniame įmonės serveryje, prie kurio gali prisijungti visi darbuotojai. Visiems jiems yra suteiktos vienodos prieigos teisės. Tam, kad būtų suteikiama darbuotojams daugiau lankstumo, yra sudaryta galimybė prisijungti prie įmonės kompiuterių nuotolinio prisijungimo programa Tight VNC viewer iš nuosavo kompiuterio. Tam naudojamas vienas bendras slaptažodis visiems darbuotojams. Šio prisijungimo trūkumas yra toks, kad norint

prisijungti nuotoliniu būdu, ofise esantis kompiuteris turi būti įjungtas, ir negali būti naudojamas kitų ofise esančių darbuotojų.

2.1.4. Duomenų apsaugos įgyvendinimas pritaikant Bendrąjį duomenų apsaugos reglamentą

Nustačius įmonės surenkamus ir naudojamus asmens duomenis bei pažeidžiamas vietas IT apsaugos srityje, įgyvendinimui pasirinkti šie Reglamento reikalavimai:

1. Su matavimais susijusių ir nesusijusių asmenų informavimas apie renkamus duomenis;
2. Duomenų apsaugos pareigūno pareigybės įsteigimas;
3. Asmens duomenų maskavimas tretiesiems asmenims siunčiamuose matavimo duomenyse;
4. Duomenų perkėlimo įgyvendinimas;
5. Teisės „būti pamirštam“ įgyvendinimas;
6. Nuotolinio prisijungimo prie tinklo saugumo stiprinimas;
7. Pranešimo apie asmens duomenų saugumo pažeidimą tvarkos nustatymas.

2.2. Duomenų subjekto informavimas apie duomenų rinkimą

Pagal Reglamento 13 straipsnį, duomenų subjektas turi būti informuojamas apie tai, kad jo duomenys bus renkami ir tvarkomi. Šiuo metu teisinis pagrindas atlikti matavimo darbus yra sutartis tarp įmonės ir užsakovo. Dažniausiu atveju užsakovas yra ir duomenų subjektas.

Nors įmonė nesiima jokių darbų savo iniciatyva, ir pirmiausia užsakovas yra suinteresuotas, kad matavimai būtų atliekami, tam, kad įmonė atitiktų Reglamento nuostatus, duomenų subjektas turi būti tinkamai informuotas apie duomenų rinkimą. Įmonėje didžiausią atliekamų darbų dalį sudaro dvi darbų rūšys: topografiniai matavimai ir kadastriniai sklypų bei pastatų matavimai.

Kadastriniuose matavimuose yra renkama ir naudojama daugiau asmens duomenų. Tuo tikslu į kadastrinių matavimų atlikimo sutartį reikia įtraukti papildomą punktą, kuris turėtų būti išdėstytas taip:

Siekdama laiku ir tinkamai atlikti Jūsų nekilnojamojo turto matavimo darbus, įmonė naudos VI „Registrų centras“ saugomus Jūsų asmens duomenis, tokius kaip vardas, pavardė, gyvenamoji vieta, bei asmens kodas, taip pat duomenis apie Jums nuosavybės teise priklausančius objektus, bei bendraturčius. Duomenys bus naudojami tik Jūsų nekilnojamojo turto registravimo dokumentacijai

paruošti ir bus saugomi tol, kol nekilnojamojo turto objektas bus įregistruotas ir visa dokumentacija bus perduota Jums.

Sutarties pavyzdys pateikiamas B priede.

Topografinių matavimų atveju asmens duomenų yra renkama ir naudojama mažiau, bet jų gali ir visai nereikėti. Tais atvejais, kai reikia nustatyti sklypo savininkus, į sutartį yra įtraukiamas tas pats papildomas punktas, kaip ir kadastrinių matavimų atveju. Jeigu nereikia nustatyti savininko duomenų, tada vieninteliai asmens duomenys, kurie yra surenkami, yra panoraminėse nuotraukose užfiksuoti vaizdai. Kadangi tai yra atsitiktiniai prasilenkiančių automobilių ar žmonių atvaizdai, būtų nepraktiška visus aplinkinius informuoti apie tai, kad matavimų metu yra užfiksuojami tam tikri jų duomenys. Tuo labiau, kad šie duomenys nebus saugomi ir naudojami kokiu nors tikslu. Tačiau, kad nekiltų teisinių klausimų, ant automobilio, su kuriuo yra atliekami matavimai, gerai matomoje vietoje turi būti užklijuotas lipdukas, informuojantis apie tai, kad šiuo automobiliu yra fotografuojama aplinka.

2.3. Duomenų apsaugos pareigūno pareigybės įsteigimas

Duomenų apsaugos pareigūnas yra Reglamente nustatyta nauja pareigybė, kuri yra atsakinga už asmens duomenų apsaugos priežiūrą įmonėje arba valstybinėje įstaigoje.

Pareigūno pagrindinės užduotys, remiantis Reglamento 39 straipsniu, yra šios:

- informuoti duomenų valdytoją arba duomenų tvarkytoją ir duomenis tvarkančius darbuotojus apie jų prievoles pagal šį Reglamentą ir kitus Sąjungos arba valstybės narės apsaugos nuostatas ir konsultuoti juos šiais klausimais;
- stebėti, kaip laikomasi šio Reglamento, kitų Sąjungos arba nacionalinės duomenų apsaugos nuostatų ir duomenų valdytojo arba duomenų tvarkytojo politikos asmens duomenų apsaugos srityje, įskaitant pareigų pavedimą, duomenų tvarkymo operacijose dalyvaujančių darbuotojų informuotumo didinimą bei mokymą ir susijusius auditus;
- paprašius konsultuoti dėl poveikio duomenų apsaugai vertinimo ir stebėti jo atlikimą pagal 35 straipsnį;
- bendradarbiauti su priežiūros institucija;
- atlikti kontaktinio asmens funkcijas priežiūros institucijai kreipiantis su duomenų tvarkymu susijusiais klausimais, įskaitant 36 straipsnyje nurodytas išankstines konsultacijas, ir prireikus konsultuoti visais kitais klausimais. [7]

Pagal Reglamento 37 straipsnį, duomenų apsaugos pareigūnas yra privalomas tik tam tikrais atvejais, kai:

- duomenis tvarko valdžios institucija arba įstaiga, išskyrus teismus, kai jie vykdo savo teismines funkcijas;
- duomenų valdytojo arba duomenų tvarkytojo pagrindinė veikla yra duomenų tvarkymo operacijos, dėl kurių pobūdžio, aprėpties ir (arba) tikslų būtina reguliariai ir sistemingai dideliu mastu stebėti duomenų subjektus;
- duomenų valdytojo arba duomenų tvarkytojo pagrindinė veikla yra specialių kategorijų duomenų tvarkymas dideliu mastu pagal 9 straipsnį ir 10 straipsnyje nurodytų asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas dideliu mastu. [7]

Kadangi nagrinėjama įmonė yra priskiriama mažų įmonių kategorijai ir neatitinka nei vieno iš aukščiau nustatytų kriterijų, asmens duomenų pareigūno pareigybės įmonėje steigti nereikia. Visa atsakomybė dėl tinkamo duomenų apsaugos užtikrinimo bei darbuotojų mokymo tenka įmonės vadovui.

2.4. Asmens duomenų maskavimas tretiesiems asmenims siunčiamuose matavimo duomenyse

Skenuojant matuojamą teritoriją, papildomai prie 3D taškų masyvo yra daromos panoraminės aplinkos nuotraukos. Nuotraukos yra naudojamos kaip pagalbinė priemonė braižytojui, padedanti geriau įvertinti ir identifikuoti matuojamoje teritorijoje esančius objektus. Tačiau papildoma informacija, tokia kaip aplinkinių pastatų adresai, praeivių veidai bei pravažiuojančių ar stovinčių automobilių registracijos numeriai, nėra reikalinga įmonės veikloje, todėl pagal Reglamento 5 straipsnį yra laikoma pertekline.

Įprastai visi matavimo duomenys yra apdorojami įmonės ofise Vilniuje ir tada siunčiami subrangovams užsienio šalyse brėžinių sudarymui. Dalis subrangovų yra Europos Sąjungos teritorijoje, dalis už jos ribų, trečiosiose pasaulio šalyse. Šioje vietoje atsiranda kita problema. Netgi jeigu papildomai užfiksuoti duomenys nebūtų laikomi pertekline informacija, tam, kad įmonė juos galėtų siųsti subrangovams už ES ribų, jie turėtų atitikti Reglamento keliamus reikalavimus. Įmonei būtų sunku užtikrinti ir kontroliuoti, kaip užsienio šalyse esančios kompanijos laikosi Reglamento reikalavimų, todėl turi būti rastas kitoks sprendimas šių duomenų siuntimui subrangovams užsienyje.

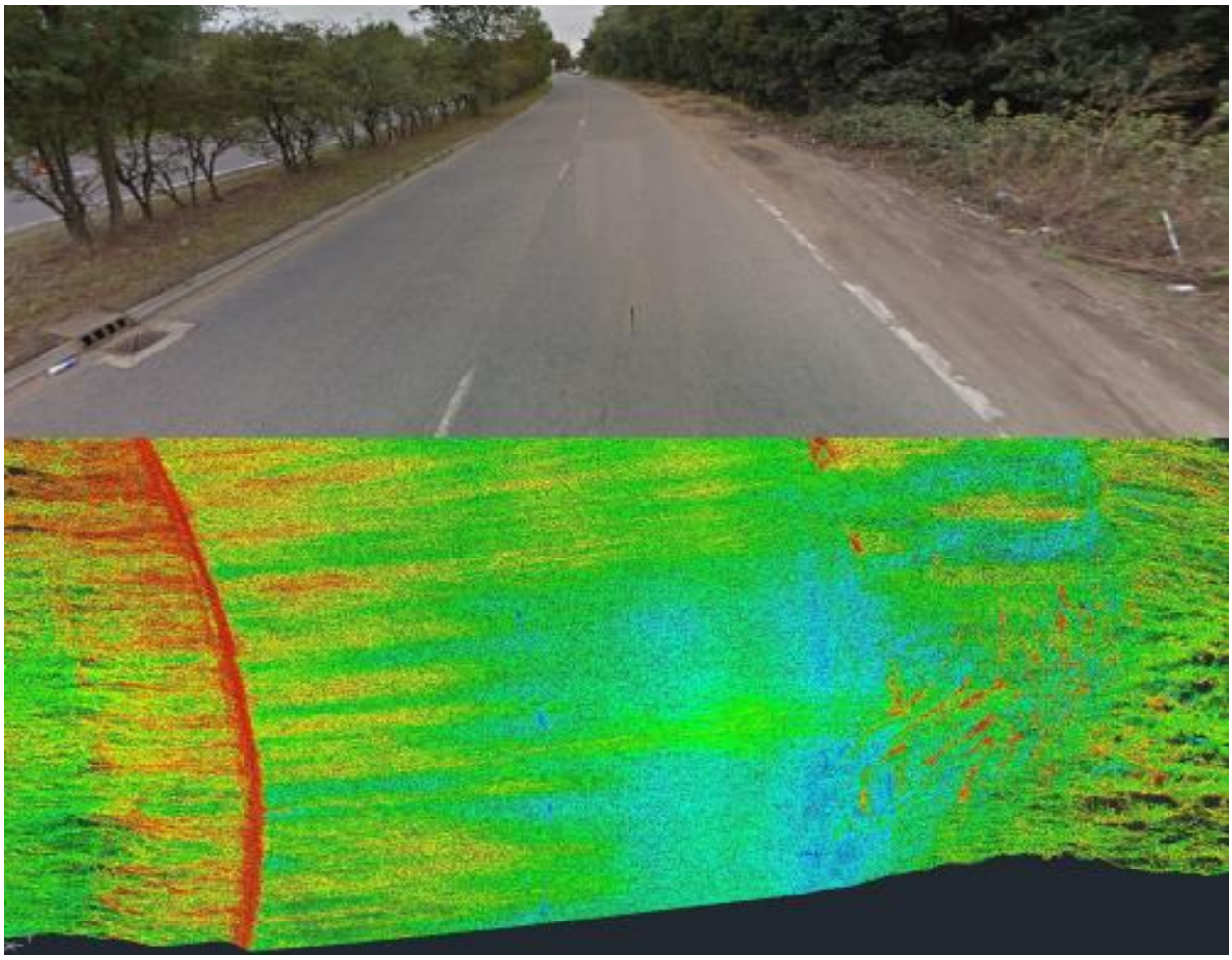
Toliau pateikiami keli problemos sprendimo būdai:

- Visiškas panoraminių nuotraukų atsisakymas;

- Nuotraukų kokybės mažinimas;
- Braižymo darbų vykdymas įmonės viduje;
- Nepageidaujamų vaizdų nuotraukose maskavimas.

2.4.1. Panoraminių nuotraukų atsisakymas

Vienas iš galimų sprendimo būdų yra visiškai atsisakyti panoraminių nuotraukų darymo. Kaip minėta anksčiau, tai yra tik pagalbinė priemonė, leidžianti geriau įvertinti aplinkos situaciją. Tačiau braižymui naudojant tik 3D taškų masyvą, atsiranda daugiau vietos interpretacijoms. Kai kurie panašūs objektai, tokie kaip skirtingų komunikacijų infrastruktūros objektai bei kelio dangos, gali būti klaidingai įvertintos ir netinkamai pažymėtos. 2.4 pav. pateikiamas pavyzdys, kaip tas pats kelio ruožas atrodo 3D taškų masyve ir panoraminėje nuotraukoje: kelkraštis ir lietaus surinkimo šulinys daug lengviau identifikuojami panoraminėje nuotraukoje.



2.4 pav. *Trimačio vaizdo ir nuotraukos palyginimas*

Tokiu atveju atliekant brėžinio kokybės patikrinimą ir nustačius netikslumus, brėžinys siunčiamas atgal subrangovui pataisymams atlikti. Vidutiniškai klaidų taisymas, įvertinus

komunikaciją ir pataisymams sugaištamą darbo laiką, gali užtrukti papildomai iki 2 dienų. Esant griežtiems darbų užbaigimo terminams, tai gali stipriai apsunkinti terminų laikymąsi. Tai savaime gali atsiliepti įmonės reputacijai prieš klientus. Dar blogiau, jeigu brėžinyje įsivėlusios klaidos nėra pastebimos kokybės patikrinimo metu. Tada brėžinys atiduodamas užsakovui su klaidomis, kurios galiausiai išryškėja tolimesniuose projektavimo etapuose. Priklausomai nuo situacijos, tai gali lemti didelius nuostolius tiek įmonei, tiek užsakovui.

2.4.2. Nuotraukų kokybės mažinimas

Panašios problemos gali kilti ir mažinant nuotraukų kokybę, nes be to, kad nuotraukose bus neatpažįstami veidai bei automobilių registracijos numeriai, gali būti sunkiai atpažįstami ir kiti, toliau nuo gatvės nutolę objektai. Šiuo atveju mažesnė tikimybė, kad tikrinimo metu klaidos bus nepastebėtos, nes tikrintojas turės nuotraukas ir galės pats įvertinti ar objektai yra pažymėti tinkamai.

2.4.3. Braižymo darbų atlikimas įmonės viduje

Dar vienas būdas išvengti asmens duomenų siuntimo į trečiąsias šalis yra visus braižymo darbus atlikti vietoje, nenaudojant subrangovų. Nusprendus visus darbus atlikti vietoje, įmonei reikėtų samdyti papildomą darbuotoją, kuris užsiimtų vien braižymu. Kadangi darbų apimtys nuolatos kinta, gali būti, kad tam darbuotojui neužteks darbo, arba, atvirkščiai, bus per didelis krūvis. Žemiau pateiktoje lentelėje palyginamos sąnaudos vykdant darbus vietoje ir samdant subrangovus.

2.1 lentelė. *Sąnaudų palyginimas*

	Įmonės darbuotojas	Subrangovas
Darbo užmokestis per dieną	45 Eur	40 Eur
Laikas brėžinio sudarymui	15 darbo dienų	3 darbo dienos
Laikas kokybės įvertinimui	1 darbo diena	2 darbo dienos
Sąnaudos vidutiniam projektui	720 Eur	200 Eur

Iš 2.1 lentelėje pateiktų duomenų galima spręsti, kad vidutinio dydžio užsakymą atliekant įmonės viduje ir samdant subrangovus, sąnaudos skiriasi beveik keturis kartus. Todėl šis būdas atmetamas kaip finansiškai nenaudingas.

2.5. Perteklinės informacijos maskavimas nuotraukose

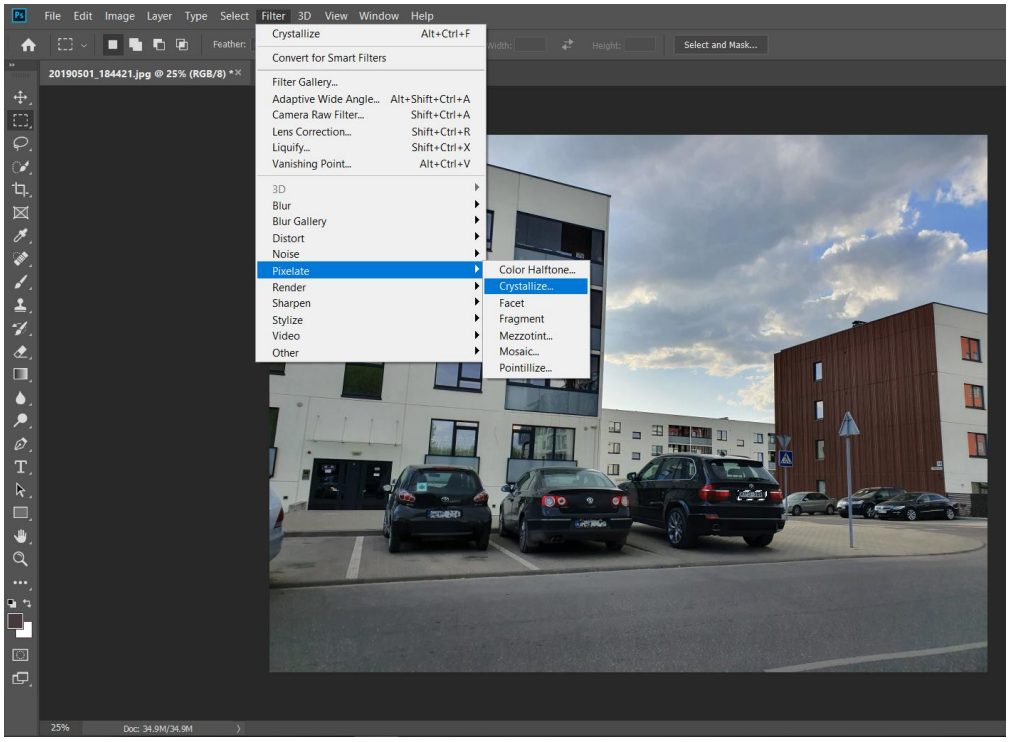
Paskutinis nagrinėjamas būdas yra perteklinių asmens duomenų nuotraukose maskavimas, pasitelkiant nuotraukų apdorojimo programas. Toliau palyginamos trys pasirinktos programos:

- Adobe Photoshop CC;
- GIMP;
- PhotoScape X.

Internetinės „*web based*“ nuotraukų koregavimo programos nebuvo vertintos dėl to, kad neredaguotų nuotraukų įkėlimas į elektroninę erdvę savaime sudaro prielaidą asmens duomenų apsaugos pažeidimui.

Šių programų pasirinkimą lėmė jų populiarumas internetinėse paieškose. Bandymuose naudota 300 nuotraukų, iš kurių 80 % buvo po vieną, 10 % po du įvairaus dydžio maskuojamus objektus, o likusiose 10 % nuotraukų nebuvo nei vieno maskuojamo objekto.

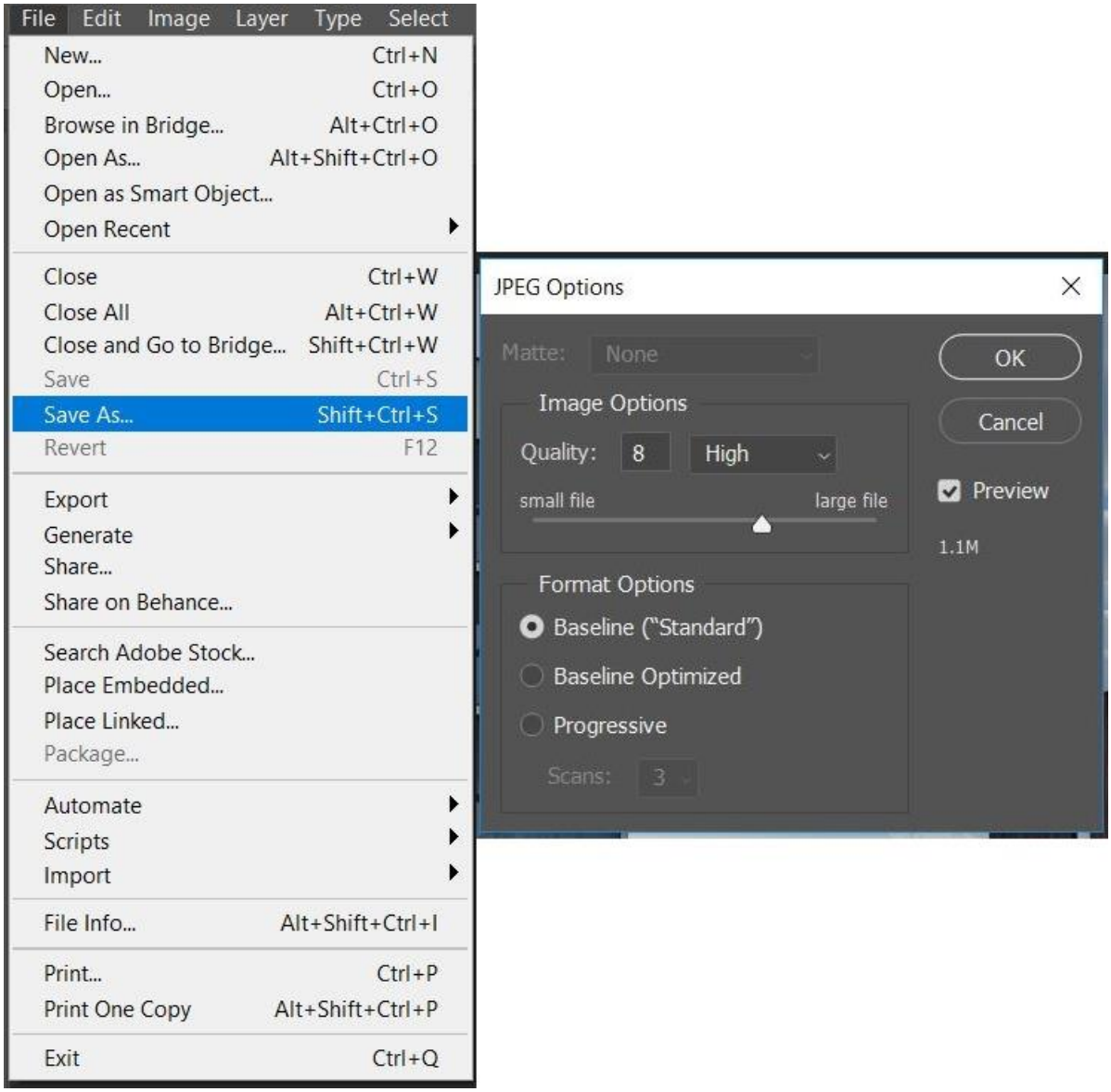
Adobe Photoshop CC yra kompanijos *Adobe* produktas, skirtas profesionaliam nuotraukų apdorojimui, dizaino kūrimui. Kadangi šioje situacijoje yra reikalinga viena gana paprasta funkcija – maskavimas (angl. *blur*), vertinamas bazinis programos variantas su mažiausiu funkcionalumu. Bazinis paketas kainuoja 144 eur/metams, perkant metinę licenciją. [14]



2.5 pav. *Photoshop pagrindinis redagavimo langas*

Nuotraukos įkeliamos į programą ir joje apdorojamos. 300 nuotraukų įkėlimo procesas trunka mažiau nei 5 minutes. Galima pasirinkti iš daugiau nei 10 maskavimo tipų. Šiuo atveju pasirinktas „*Pixelate*“ maskavimo tipas. Pagrindinis programos langas pateikiamas 2.5 pav.

Pirmiausia pasirinkta forma (ovalu arba kvadratu) pažymima vieta, kurioje yra maskuojamas objektas, o tada pasirenkama maskavimo funkcija. Pereinant prie kitos nuotraukos kas kartą reikia įrašyti kiekvieną nuotrauką atskirai, pasirenkant nustatymus kiekvienai nuotraukai (2.6 pav.), nesvarbu, ar joje buvo kas nors pakeista, ar ne. Pasirinkimo, kad įsimintų prieš tai naudotus nustatymus, nėra. Įrašant visas nuotraukas vienu metu pabaigus redagavimą, yra išsaugomos ne atskiros nuotraukos, o Photoshop projektas, kuris reikalautų tolesnio apdorojimo.



2.6 pav. *Photoshop CC įrašymo langas*

Privalumas yra tas, kad jeigu išsaugojus ir perėjus prie kitos nuotraukos nėra pasirenkamos jokios naujos funkcijos, tada programa įsimena ir iš karto leidžia naudoti paskutinę naudotą funkciją, tai yra, nereikia kaskart ieškoti meniu juostoje maskavimo funkcijos.

Atlikus redagavimą ir įrašius visas nuotraukas, jų bendras dydis sumažėjo apytiksliai 25 %, tai reiškia, kad nuotraukų kokybė sumažėjo ketvirtadaliu. Tiesa, vizualiai peržiūrėjus nuotraukas, akivaizdaus kokybės pablogėjimo nepastebėta. Nuotraukos pavyzdys prieš ir po redagavimo pateikiamas 2.7 pav. Visas 300 nuotraukų redagavimo procesas, neskaitant įkėlimo, truko apie valandą.



2.7 pav. *Nuotrauka prieš ir po redagavimo Photoshop programa*

GIMP yra laisvai prieinama, nemokama vaizdų apdorojimo ir dizaino kūrimo programa, sukurta kaip alternatyva mokamam *Adobe Photoshop* produktui su sąlyginai mažesniu funkcionalumu. [9] Tačiau kaip minėta anksčiau, šioje situacijoje nereikalingos kokios nors ypatingos funkcijos, todėl programa visiškai tinka šiam darbui.

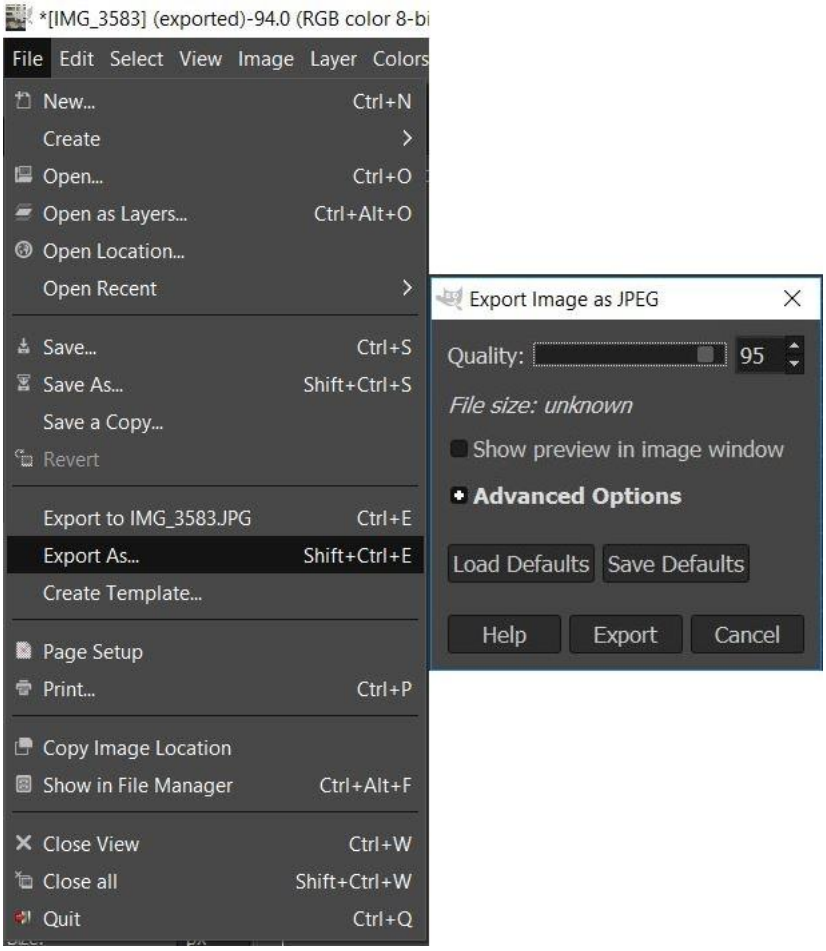
Pagrindinė darbo seka labai panaši į Photoshop CC. Nuotraukos įkeliamos į programą ir joje redaguojamos. Įkelti tas pačias 300 nuotraukų trunka apie 15 minučių. Maskavimo procesas toks pat kaip ir Photoshop CC, nereikia atlikti papildomų žingsnių. Programa įsimena paskutinę naudotą funkciją ir kitai nuotraukai galima ją panaudoti greičiau. Pagrindinio nuotraukos redagavimo lango pavyzdys pateikiamas 2.8 pav.



2.8 pav. *Pagrindinis GIMP redagavimo langas*

Šiek tiek skiriasi redaguotų nuotraukų įrašymas. Nuotraukas galima įrašyti iškart redagavus arba užbaigus visų nuotraukų redagavimą. Pasirinkus įrašymo funkciją, išsaugoma GIMP standartiniu .xcf formatu. Norint išsaugoti originaliu nuotraukos formatu, reikia rinktis eksportavimo funkciją ir,

pasirinkus parametrus, eksportuoti kiekvieną nuotrauką atskirai (2.9 pav.). Lyginant su Photoshop CC, čia prisideda pora papildomų žingsnių.



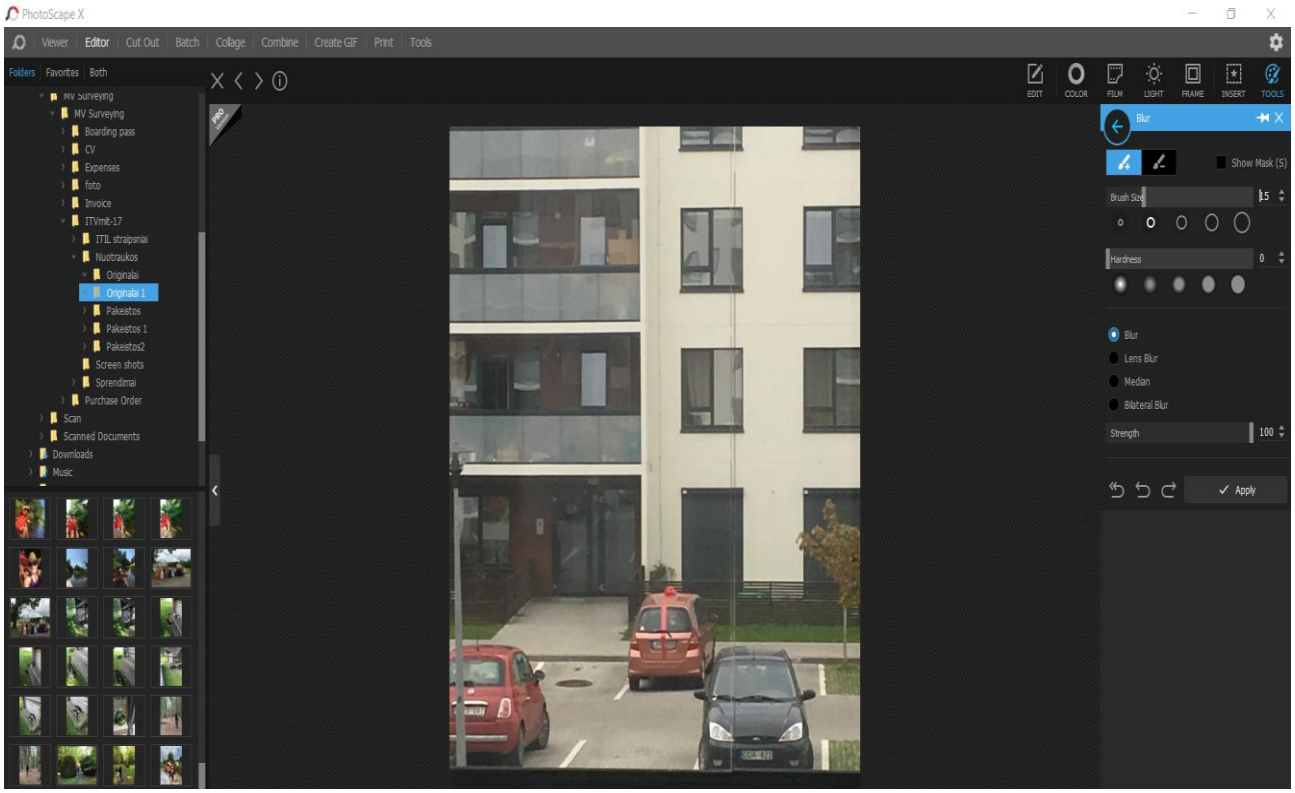
2.9 pav. *GIMP failo eksportavimo langas*

Skirtingai nei Photoshop CC programoje, baigus visų nuotraukų redagavimą, visų nuotraukų dydis nepasikeičia, vadinasi kokybės sumažėjimo nėra. Tiesa, apdoroti ir įrašyti visas nuotraukas trunka daugiau nei dvi valandas, o tai yra dvigubai ilgiau nei Photoshop CC programa.

PhotoScape X tai *Mooii Tech* kompanijos vaizdų ir video apdorojimo programa. Galima įsigyti nemokamą arba PRO versiją. [13] Kadangi nemokama versija turi pakankamą funkcionalumą, mokama versija nevertinta.

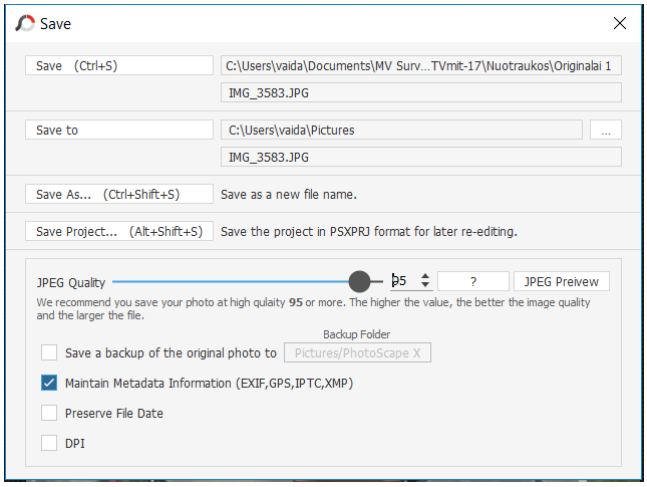
Skirtingai nuo ankstesnių dviejų redagavimo programų, PhotoScape X nereikia nuotraukų įkelti į programą. Tam, kad būtų galima redaguoti nuotraukas, užtenka nurodyti aplanką, kuriame yra redaguojamos nuotraukos, ir galima paeiliui su jomis visomis dirbti. Pasirinkus maskavimo (*blur*) funkciją nereikia prieš tai pažymėti norimos maskuoti vietos. Maskavimas vyksta panašiai kaip pieštuko ar teptuko principu – priklausomai nuo maskuojamo objekto dydžio, pasirenkamas žymeklio

dydis ir užmaskuojama ta vieta, kuri buvo pažymėta kompiuterio pele. Nuotraukų redagavimo lango pavyzdys - 2.10 pav.



2.10 pav. *PhotoScape X programos redagavimo langas*

Kadangi nuotraukose veidai ir automobilių registracijos numeriai yra panašaus dydžio, tai palyginus su Photoshop CC ir GIMP programomis, šioje programoje reikalingas minimalus žingsnių skaičius. Kadangi nuotraukos nėra įkeltos į programą, kiekvieną kartą pereinant prie kitos nuotraukos ją reikia įrašyti.



2.11 pav. *Nuotraukos įrašymo langas*

Palyginus su ankstesnėmis programomis, įrašymo dialoge yra tik du žingsniai: pasirinkti įrašymo mygtuką ir pasirinkti, ar norima užrašyti ant jau egzistuojančio failo, ar sukurti naują (2.11 pav.).

Privalumas dar ir tai, kad jeigu nuotrauka nebuvo pakeista, jos nereikia išsaugoti, nes ir pakeistos ir nepakeistos nuotraukos yra tame pačiame aplanke.

Pabaigus visų nuotraukų redagavimą, viso aplanko dydis liko nepakitęs, tai reiškia, kad kokybės praradimo nebuvo. Visas 300 nuotraukų užmaskuoti ir išsaugoti trunka mažiau nei valandą.

2.2 lentelėje pateikiamas programų naudingumo vidutiniam matavimų projektui palyginimas. Vidutinis matavimo projektas su aukštos kokybės nuotraukų nustatymais sudaro apie 1000 nuotraukų.

2.2 lentelė. *Vaizdų redagavimo programų palyginimas*

Kriterijus/Programa		Photoshop CC	GIMP	PhotoScape X
Nuotraukų kokybės praradimas		25%	0%	0%
Patogumas vartotojui	Žingsnių skaičius vienai nuotraukai	<5	<5	2
	Nuotraukų įrašymas	<5	<5	2
Kompiuterių resursų naudojimas		Galima vykdyti kitas operacijas	Maksimalus naudojimas	Galima vykdyti kitas operacijas
Pagalbos prieinamumas		Forumas, gyvas pokalbis, el. paštas	Forumas, el. paštas	Forumas, video pamokos,el. paštas
Darbo greitis		iki 0,5 darbo dienos	apie 1 darbo dieną	iki 3 valandų
Kaina		144 eur/metams	Nemokama	Nemokama

Taigi, įvertinus visus galimus pasirinkimus galima teigti, kad įmonei naudingiausia naudoti perteklinių vaizdų maskavimo procesą. Įmonės prioritetas yra gauti kuo kokybiškesnius brėžinius iš subrangovų, todėl nei nuotraukų atsisakymas, nei kokybės mažinimas netinka. Finansine prasme, brėžinių sudarymo įmonės viduje kaštai yra kelis kartus didesni nei papildomam darbo laikui, būtinam nuotraukoms redaguoti prieš siunčiant jas subrangovui.

Pagal 2.2 lentelėje pateiktus kriterijus iš visų lygintų programinių paketų naudingiausia įmonei būtų naudoti nemokamą PhotoScape X versiją, todėl, kad:

- programa apdorojus nuotraukos, jos kokybė nepakinta;
- programos valdymas paprastas, o apdorojimui reikalingas minimalus žingsnių skaičius;

- programa nenaudoja maksimalių kompiuterio resursų, todėl galima vykdyti kitas užduotis tuo pačiu metu;
- užduotys atliekamos greitai, o prireikus pagalbos yra daug įvairių nuotolinės pagalbos vartotojams priemonių.

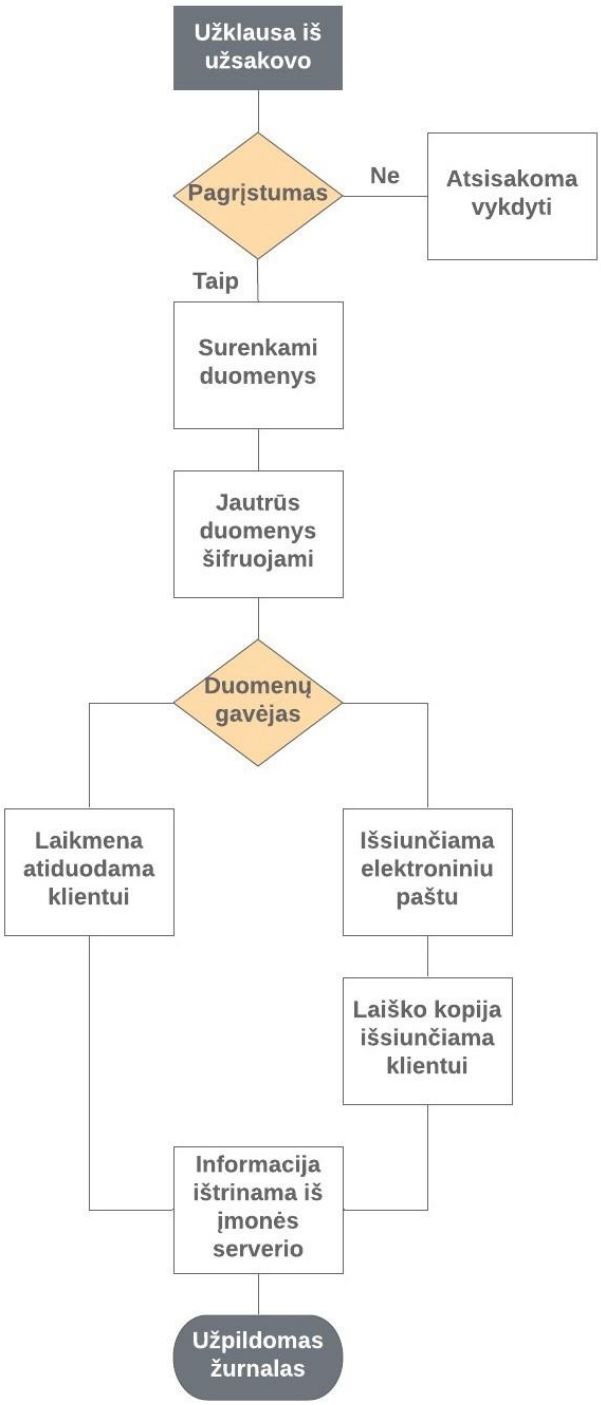
2.6. Duomenų perkeliamumo įgyvendinimas

Bendrojo duomenų apsaugos reglamento 20 straipsnio 1 dalis numato, kad, klientui pareikalavus, visi duomenys, kuriuos įmonė turi apie klientą, būtų jam pateikti arba perduoti kitam duomenų valdytojui.

Priklausomai nuo matavimo darbų kompleksiškumo ir matuojamos teritorijos dydžio, darbai gali užtrukti nuo vienos dienos iki mėnesio ar net kelių. Jeigu darbų vykdymo metu klientas dėl tam tikrų priežasčių nuspręstų nutraukti sutartį su įmone ir perduoti darbų atlikimą kitam vykdytojui, pagal reglamento nuostatus įmonė turėtų nesudaryti kliūčių duomenų perkėlimui. Tai gali būti padaryta dviem būdais:

- perduoti duomenis klientui – tokiu atveju klientas būtų pats atsakingas už duomenų perdavimą kitam jo pasirinktam vykdytojui;
- persiųsti visus duomenis tiesiai kliento pasirinktam naujam vykdytojui.

Duomenų perdavimo procesas pavaizduotas 2.12 pav.



2.12 pav. *Duomenų perkėlimo procesas*

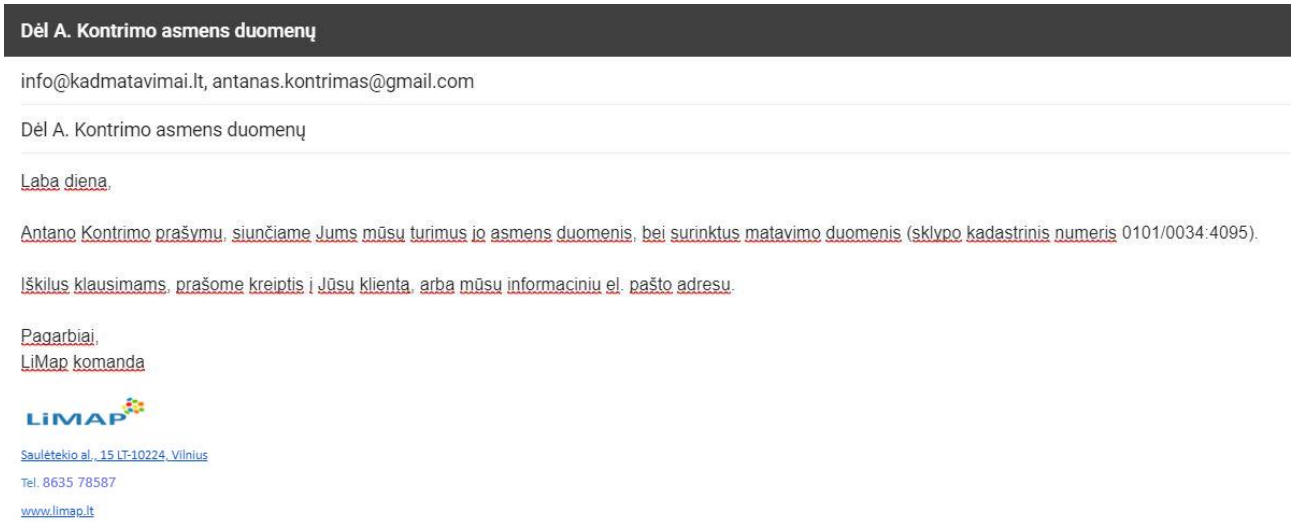
Klientui pateikus užklausą dėl jo asmens duomenų perkėlimo, įmonės vadovas ją įvertina ir nusprendžia, ar ji pagrįsta ar ne. Kadangi Reglamentas įpareigoja perduoti duomenis klientui to pareikalavus, vienintelis kriterijus, dėl kurio įmonė gali atsisakyti perduoti duomenis, yra teisėti įmonės interesai į apmokėjimą už atliktus darbus pagal sutartį, nes Reglamento 20 straipsnio 4 dalis teigia, kad *1 dalyje nurodyta teisė negali daryti neigiamo poveikio kitų teisėms ir laisvėms* [7]. Jeigu

visi kliento ir įmonės sutarties punktai yra įvykdyti, priimamas sprendimas tenkinti kliento užklausą. Sekančiame etape atsakingas darbuotojas surenka visą įmonės turimą informaciją apie klientą:

- visus surinktus matavimo duomenis, kurie nėra intelektinė įmonės nuosavybė;
- kliento asmens duomenis.

Surinkus visą turimą informaciją apie klientą, ji yra skirstoma į jautrią informaciją ir nejautrią. Siekiant apsaugoti jautrią informaciją nuo netyčinio atskleidimo ar nutekėjimo perdavimo procese, tokia informacija yra šifruojama.

Užšifruoti duomenys ir nešifruoti matavimo duomenys pagal susitarimą su užsakovu gali būti perduoti jam pačiam arba persiųsti kliento pasirinktam naujam užsakovui. Jeigu klientas pageidauja gauti duomenis pats, jie yra įrašomi į jam priklausančią USB ar HDD laikmeną arba atsiunčiama elektroniniu paštu. Klientui pageidaujant, kad duomenys būtų perduoti tiesiai kitam vykdytojui, įmonė persiunčia duomenis naudodama elektroninį paštą, o jeigu failų dydis viršija elektroninio pašto tiekėjo nustatytą limitą - įkelia juos į savo *Google Drive* paskyrą ir suteikia prieigą prie failų naujam vykdytojui. Elektroninio laiško kopija, kaip įrodymas, nusiunčiama ir klientui. Standartinio laiško pavyzdys pateikiamas 2.13 pav.



2.13 pav. *Laiško naujam vykdytojui šablonas*

Atskiru elektroniniu laišku, trumpąja žinute ar, bendraujant tiesiogiai, žodžiu, klientui yra perduodamas slaptažodis, reikalingas iššifruoti perduotus kliento asmens duomenis.

Perdavus kliento duomenis, likusios dokumentų kopijos negrįžtamai sunaikinamos, o perkėlimo ir sunaikinimo faktas užfiksuojamas įmonės žurnale kaip įrodymas, jeigu ateityje būtų vykdomas įmonės auditas duomenų apsaugos srityje.

2.7. Teisės būti pamirštam įgyvendinimas

Bendrojo duomenų apsaugos reglamento 17 straipsnyje numatyta kliento teisė pareikalauti, kad duomenų valdytojas ištrintų visus saugomus ir naudojamus duomenis apie jį, kitaip vadinama teisė būti pamirštam.

Atlikus matavimo darbus ir atidavus galutinį produktą užsakovui, įmonė turimus duomenis saugo tiek laiko, kiek yra aktualūs matavimo rezultatai. Topografinių matavimų atveju tai yra vieneri metai, kadastrinių matavimų atveju – tol, kol žemės sklypas ar statinys yra užregistruojamas.

Šiame darbe nėra nagrinėjamas finansinių ir administracinėje veikloje naudojamų duomenų sunaikinimas, nes tokiems duomenims galioja papildomi reikalavimai ir dėl jų gali kilti teisinių klausimų.

Jeigu dėl tam tikrų priežasčių klientas nuspręstų, kad nenori, jog jo asmens duomenys būtų saugomi iki numatyto termino, Reglamentas įpareigoja įmonę pageidavimą įvykdyti.

Teisės būti pamirštam įgyvendinimo procesas pavaizduotas 2.14 pav.

Jeigu klientas nusprendžia, kad nori, jog visi jo duomenys, kuriuos turi surinkusi įmonė, būtų ištrinti nesibaigus nustatytam matavimo duomenų aktualumo terminui, jis pateikia prašymą įmonei. Įmonės vadovas įvertina, ar prašymas pagrįstas, tai yra, ar tenkinama bent viena iš Reglamento 17 straipsnio 1 dalyje numatytų sąlygų:

- asmens duomenys nebėra reikalingi, kad būtų pasiekti tikslai, kuriais jie buvo renkami arba kitaip tvarkomi;
- asmens duomenų subjektas atšaukia sutikimą, kuriuo pagal 6 straipsnio 1 dalies a punktą arba 9 straipsnio 2 dalies a punktą grindžiamas duomenų tvarkymas ir nėra jokio kito teisinio pagrindo tvarkyti duomenis;
- asmens duomenų subjektas nesutinka su duomenų tvarkymu pagal 21 straipsnio 1 dalį ir nėra viršesnių teisėtų priežasčių tvarkyti duomenis arba duomenų subjektas nesutinka su duomenų tvarkymu pagal 21 straipsnio 2 dalį;
- asmens duomenys buvo tvarkomi neteisėtai;
- asmens duomenys turi būti ištrinti laikantis Sąjungos arba valstybės narės teisėje, kuri taikoma duomenų valdytojui, nustatytos teisinės prievolės;
- asmens duomenys buvo surinkti 8 straipsnio 1 dalyje nurodyto informacinės visuomenės paslaugų siūlymo kontekste. [7]

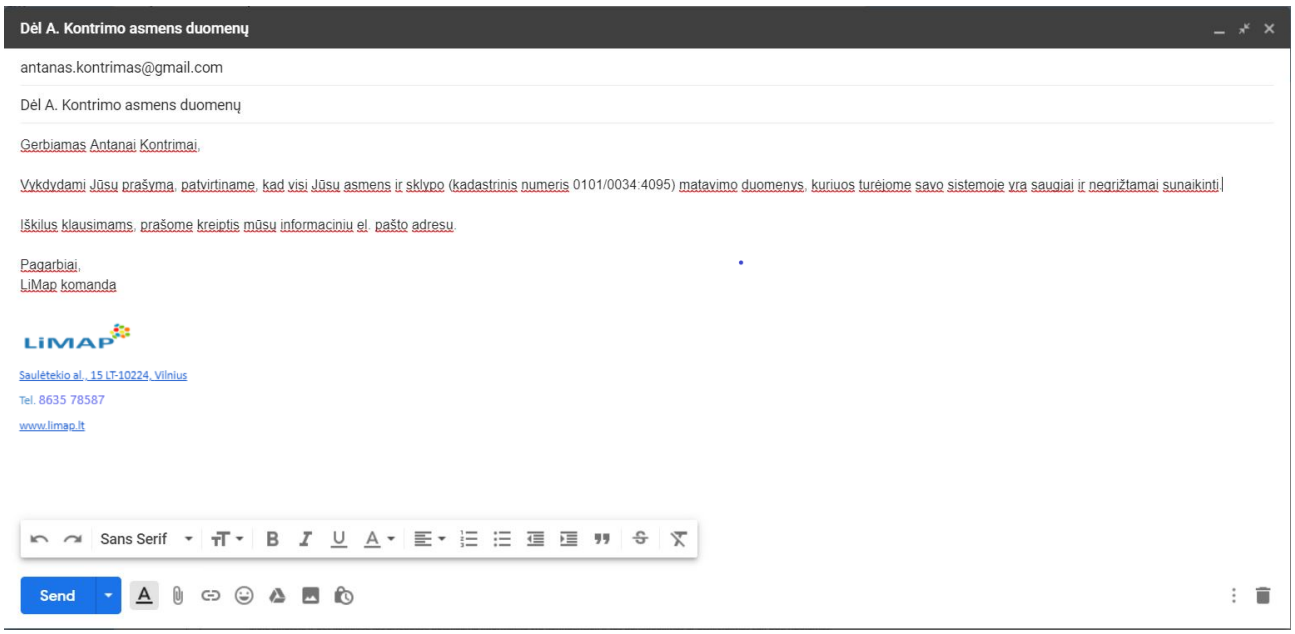


2.14 pav. *Teisės būti pamirštam procesas*

Jeigu šios sąlygos tenkinamos, vadovas paveda atsakingam darbuotojui atlikti tolimesnius veiksmus. Priešingu atveju, prašymą tenkinti atsisakoma apie sprendimą pranešant klientui standartiniu elektroniniu laišku.

Gavęs pavedimą iš vadovo, atsakingas darbuotojas patikrina, ar kliento duomenys vis dar egzistuoja įmonės sistemose. Surinkus visus duomenis, jie yra suskirstomi į jautrius asmens duomenis ir matavimo duomenis. Siekiant užtikrinti, kad duomenų nebūtų galima ateityje atstatyti, jie yra negrįžtamai sunaikinami specialia programine įranga. Matavimo duomenys yra ištrinami.

Atlikus duomenų naikinimo darbus, yra išsiunčiamas standartinis elektroninis pranešimas klientui (2.15 pav.), patvirtinantis, kad jo duomenys yra sėkmingai sunaikinti. Taip pat yra užpildomas įmonės žurnalas tam atvejui, jeigu įmonėje būtų atliekamas duomenų apsaugos auditas.



2.15 pav. *Duomenų sunaikinimo patvirtinimo laiško šablonas*

2.8. Jautrios informacijos šifravimo ir negrįžtamo naikinimo programų palyginimas

Siekiant apsaugoti perduodamus duomenis nuo nutekėjimo ir netyčinio atskleidimo, jautrūs duomenys yra šifruojami. Taip pat tam, kad klientui pareikalavus jo duomenys būtų saugiai ir negrįžtamai pašalinti iš įmonės serverių, yra reikalinga programinė įranga negrįžtamam sunaikinimui. Šioje dalyje palyginamos trys pasirinktos šifravimo programos:

- SensiGuard;
- Secure IT;
- 7-Zip File Manager.

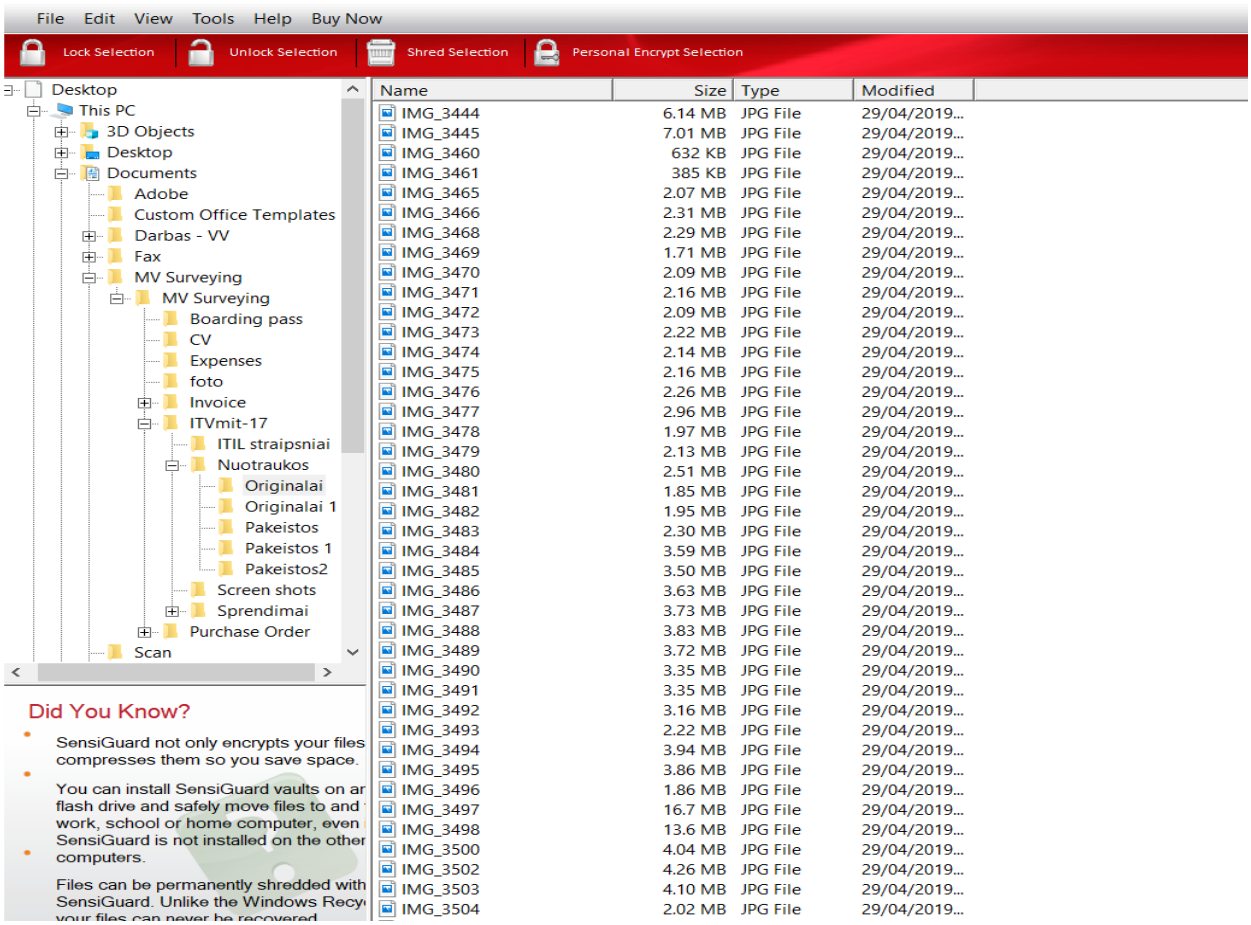
Taip pat buvo įvertinama galimybė atlikti negrįžtamą sunaikinimą šiomis programomis. Programos pasirinktos dėl jų populiarumo internetinėse paieškose. Asmens duomenų failų apimtis dažniausiai būna maža, todėl ir bandymuose naudoti nedidelės apimties failai.

SensiGuard yra amerikiečių kompanijos *WebMinds* sukurta programinė įranga, skirta failams šifruoti ir naikinti. Tai yra komercinis produktas, kurio licencija vienam kompiuteriui kainuoja apie 30 eurų. [18]

Pirmą kartą paleidžiant programą vartotojas yra prašomas susikurti slaptažodį, kuris bus naudojamas kaip iššifravimo raktas. Kitaip nei daugelyje kitų šifravimo programų, SensiGuard yra funkcija, skirta atstatyti pamirštą slaptažodį. Tam galima pasirinkti tris klausimus ir atsakymus į juos, kurie bus naudojami, kreipiantis dėl pamiršto slaptažodžio.

Programos vartotojo sąsaja panaši į Microsoft Windows operacinių sistemų naršykles. Tai leidžia vartotojui greičiau perprasti programos veikimą. Gali būti šifruojami atskiri failai arba aplankai. Naršyklėje pasirinkus norimą failą arba aplanką užtenka iš meniu juostos pasirinkti norimą veiksmą: šifruoti, iššifruoti ar ištrinti (2.16 pav). Programa šifruodama duomenis automatiškai suglaudina failus, kad būtų galima sutaupyti papildomos vietos diske. Iššifravimas vyksta identiškai, tik pasirenkama funkcija – iššifruoti. Ši programa yra labiau skirta failų šifravimui asmeniniais tikslais, siekiant apsaugoti kompiuteryje esančius duomenis. Šifruojant duomenis programa nesukuria šifruotos failo ar aplanko kopijos, o užšifruoja patį failą. Tai tinka naudojimui asmeniniame kompiuteryje, bet apsunkina dalijimąsi failais su kitais asmenimis. Norint, kad kiti asmenys galėtų atidaryti tuos pačius failus, programoje yra sukuriamas šifravimo raktas, kuris turi būti perduotas kitam asmeniui kartu su šifruotu failu.

Dar viena kliūtis trukdanti sklandžiai parduoti šifruotus duomenis yra tai, kad gavėjas turi turėti tokią pačią programinę įrangą savo kompiuteryje. Kadangi programa yra mokama, tai sukeltų papildomų kaštų klientui arba naujam vykdytojui.



2.16 pav. *SensiGuard pagrindinis langas*

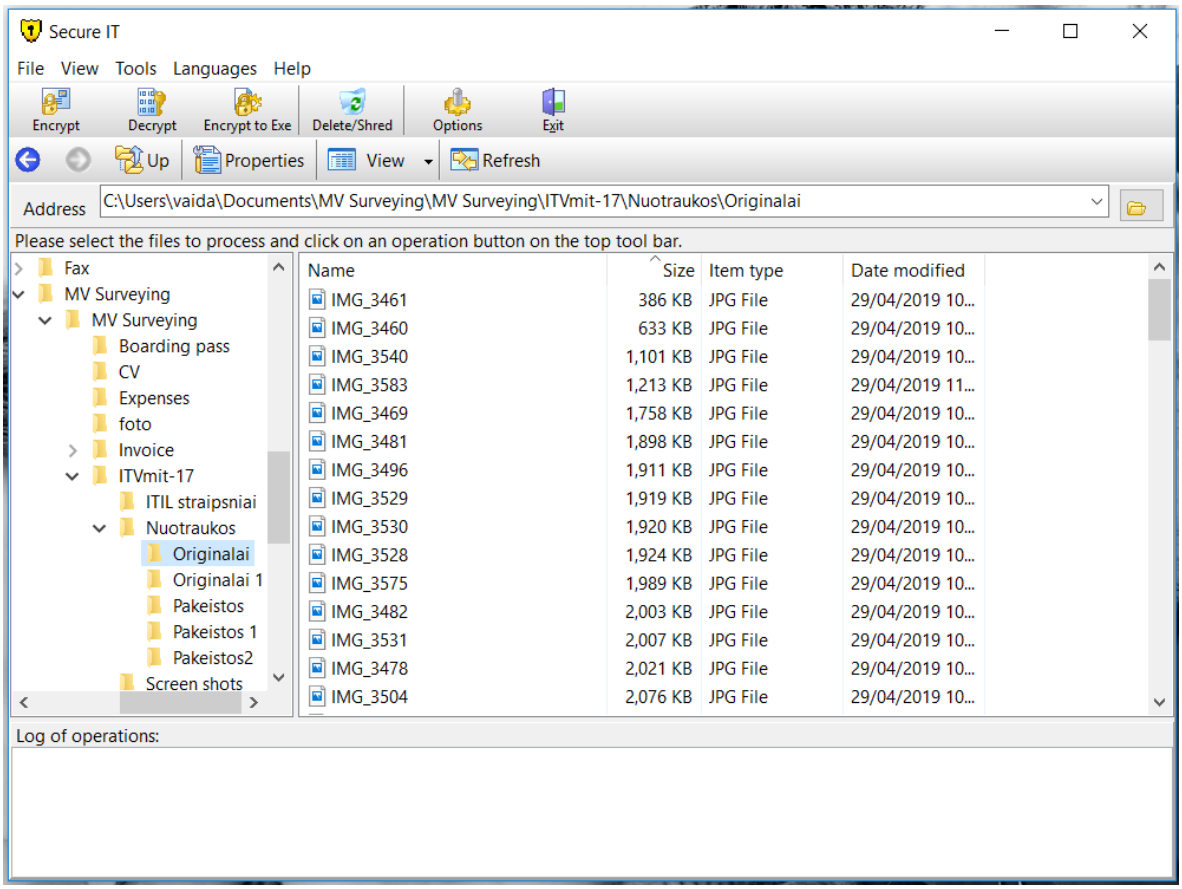
Trečioji programinės įrangos funkcija yra failų naikinimas negrįžtamai. Tai gali būti naudojama įgyvendinant Reglamento nuostatą, numatančią teisę klientui pareikalauti, kad duomenų valdytojas pašalintų visus turimus jo asmeninius duomenis iš savo sistemų.

Secure IT yra Indijos kompanijos Cypherix produktas, skirtas šifruoti ir trinti failus. Vienos licencijos kaina yra 35 eurai. [17]

Skirtingai nei SensiGuard produkte, Secure IT nereikalauja vartotojo susikurti vieno slaptažodžio. Ši programa labiau orientuota į dalinimąsi failais. Vartotojo sąsaja panaši kaip ir prieš tai aprašytoje programoje, priderinta prie Windows operacinių sistemų (2.17 pav.).

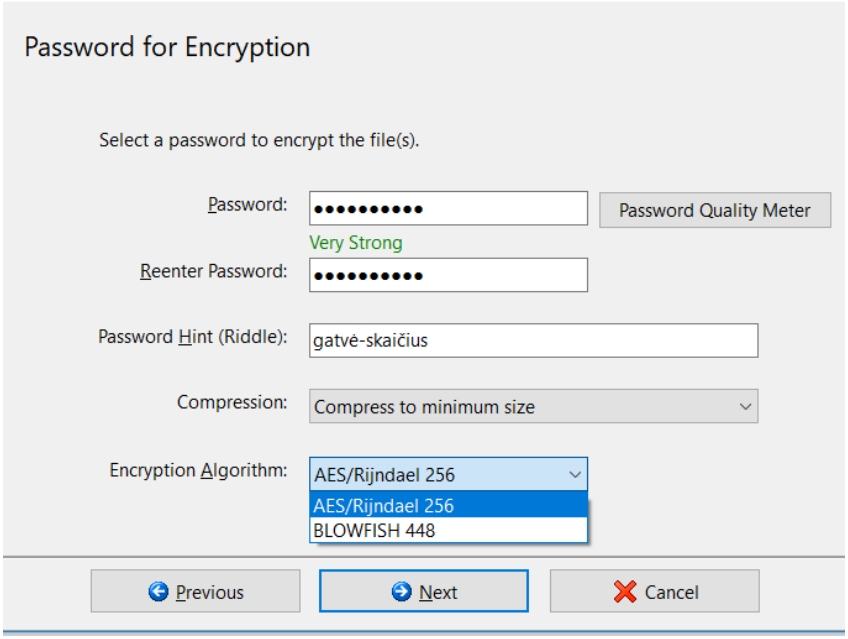
Programos pagrindą sudaro keturios pagrindinės funkcijos:

- Šifravimas;
- Dešifravimas;
- Šifravimas išoriniams vartotojams;
- Sunaikinimas.

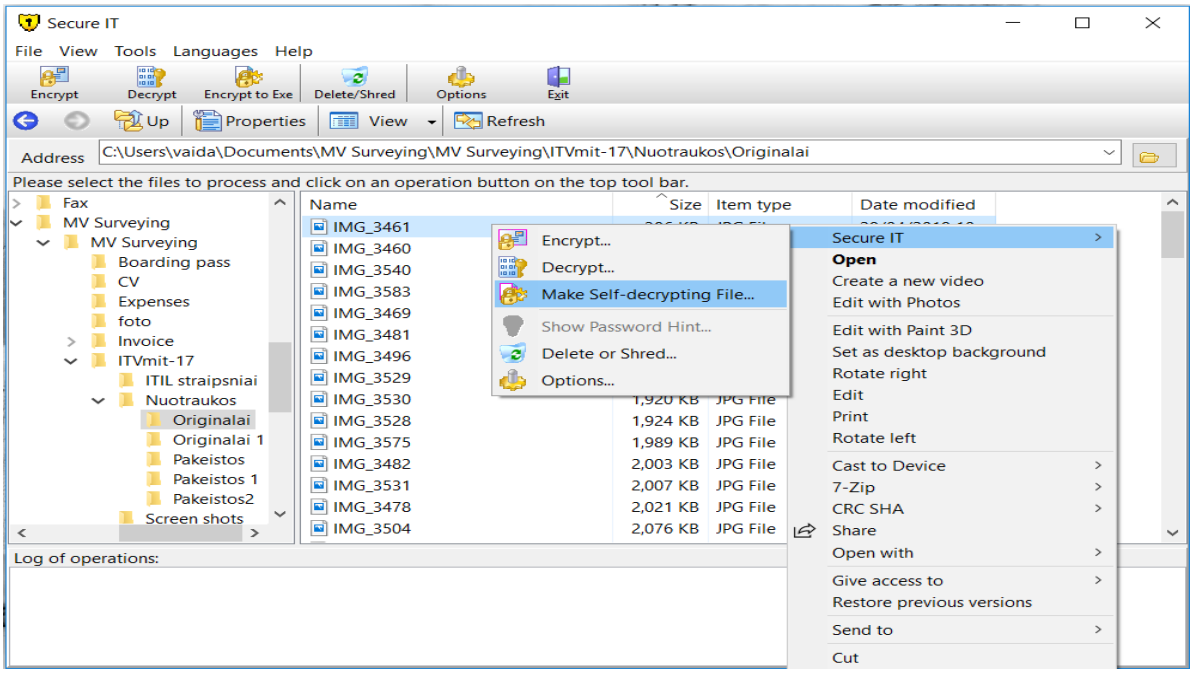


2.17 pav. *Pagrindinis Secure IT meniu langas*

Šifruojant dokumentus vartotojas turi sukurti vienkartinį slaptažodį, kuris bus naudojamas dešifruoti būtent tą dokumentą. Taip pat galima pasirinkti šifravimo būdą: AES arba BLOWFISH (2.18 pav.).



2.18 pav. *Slaptažodžio su užuomina kūrimas*



2.19 pav. *Šifravimas išoriniams vartotojams*

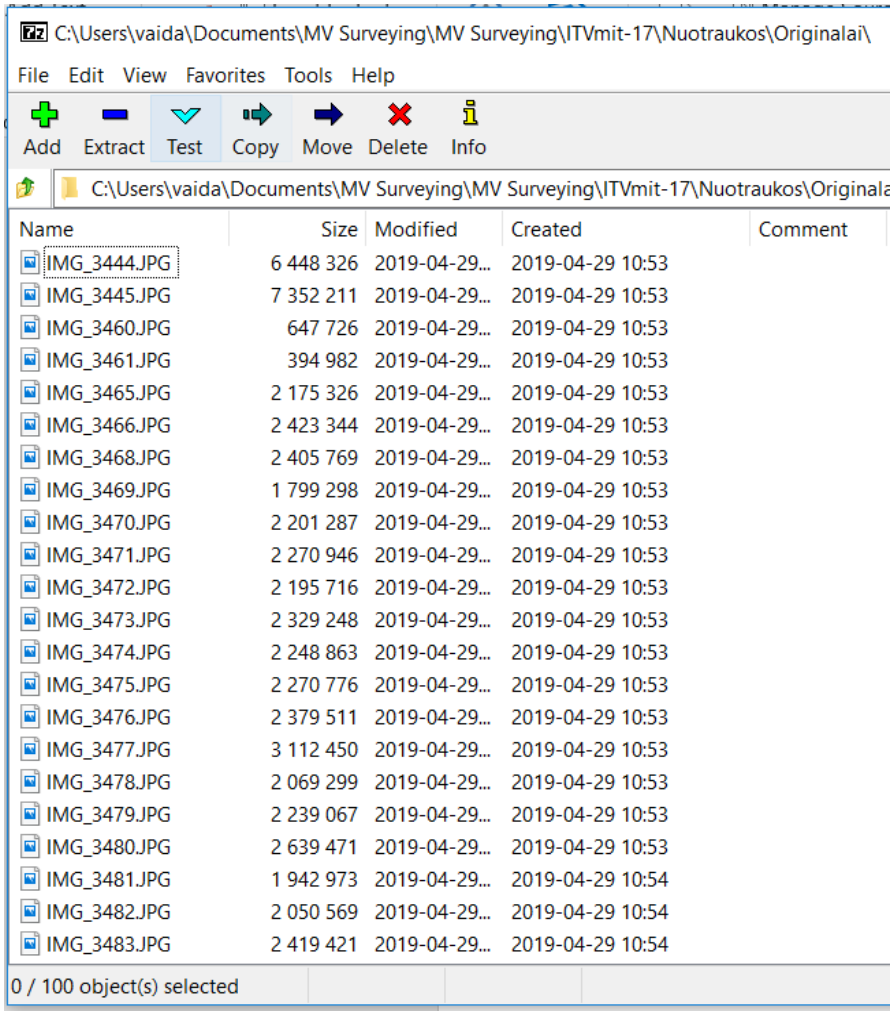
Skirtingai nei prieš tai nagrinėtoje programoje, Secure IT yra galimybė šifruoti dokumentus išorinių klientų naudojimui (2.19 pav.). Tam yra du būdai: šifruoti į failą nereikalaujantį jokios programinės dešifravimo įrangos arba į failą, dešifruojamą nemokama Secure IT programine įranga.

Abiem šiais atvejais vartotojas turi sukurti slaptažodį, skirtą tam failui ir jį perduoti klientui. Kliento patogumui galima sukurti slaptažodžio užuominą. Nagrinėjamu atveju tai gali būti užuomina, žinoma tiek įmonei tiek klientui, pavyzdžiui „objekto adresas“ (2.18 pav.). Taip būtų išvengiama būtinybės perduoti klientui slaptažodį.

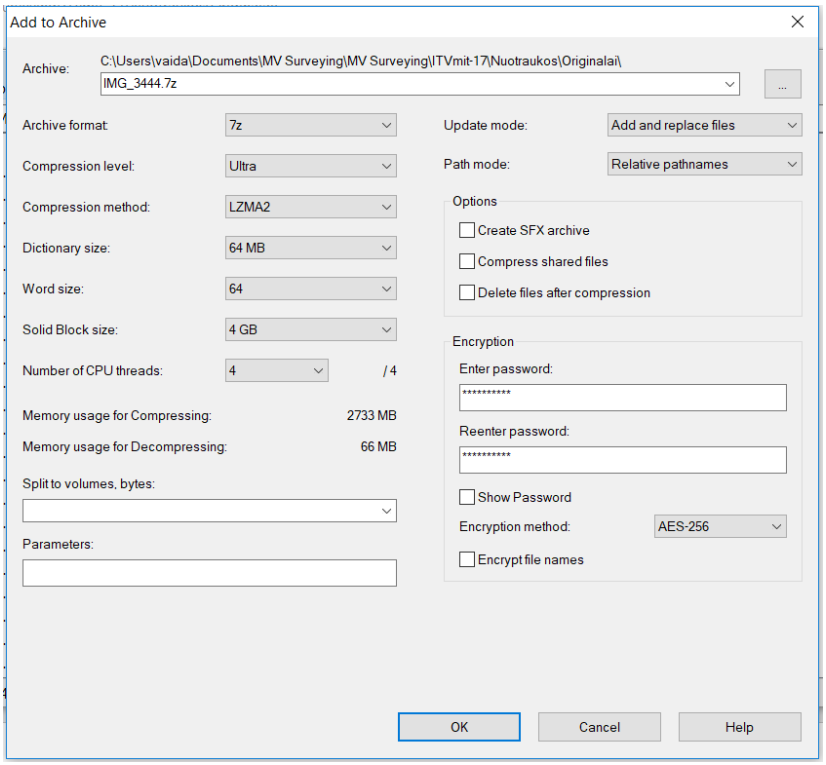
Programoje taip pat yra galimybė sunaikinti failus negrįžtamai tam, kad jų nebūtų galima atstatyti net su dokumentų atstatymo programomis.

7-Zip File Manager yra atviro kodo nemokama programa. [22] Jos pagrindinė funkcija yra lengvai grupuoti didelius kiekius failų į vieną failą, vadinamą archyvu.

Kaip ir Secure IT, ši programinė įranga nereikalauja susikurti vartotojo paskyros. Microsoft Windows naršyklės tipo lange (2.20 pav.) pasirinkus norimą failą ar aplanką, pasirenkama archyvavimo funkcija ir atsidariusiame lange pasirenkamas glaudinimo stiprumas ir, šifravimo atveju, norimas slaptažodis (2.21 pav.).



2.20 pav. *Pagrindinis 7-Zip File Manager meniu langas*



2.21 pav. *Glaudinimo ir slaptažodžio pasirinkimo langas*

Visi šia programa užšifruoti dokumentai gali būti dešifruojami standartiniu Windows operacinėje sistemoje esančiu dešifravimo įrankiu. Skirtingai nei Secure IT atveju, tam nereikia papildomai keisti šifravimo nustatymų.

Taip pat yra galimybė nustatyti, kad užšifravus duomenis jie būtų išsiųsti norimu elektroninio pašto adresu.

Priešingai nei kitos dvi aukščiau aprašytos programinės įrangos, 7-Zip File Manager neturi funkcijos negrįžtamai naikinti failų.

Žemiau pateikiama skirtingų šifravimo programinių įrangų palyginimo lentelė.

2.3 lentelė. *Šifravimo programų palyginimas*

Kriterijus/Programa		SensiGuard	Secure IT	7-Zip File Manager
Galimybė dešifruoti failus be specialios programinės įrangos		Nėra	Yra	Yra
Galimybė sukurti vienkartinį slaptažodį		Nėra	Yra	Yra
Patogumas vartotojui	Žingsnių skaičius dokumento šifravimui	1	4	3
	Žingsnių skaičius dešifruojant	2	2	2
Paliekamas originalus failas		Ne	Taip	Taip
Galimybė negrįžtamai naikinti failus		Yra	Yra	Nėra
Pagalbos prieinamumas		Vartotojo vadovas, el. paštas	Vartotojo vadovas, el. paštas	Forumas, dažniausi klausimai
Kaina		30 Eur	40 Eur	Nemokama

Vertinant 2.3 lentelėje pateiktus kriterijus matome, kad naudingiausia įmonei yra naudoti Secure IT programinę įranga, nes:

- Ją galima naudoti tiek failų šifravimui, tiek failų negrįžtamam naikinimui;
- Dešifruojant failus nėra būtinybės turėti dešifravimo programinę įrangą;
- Šifruojant yra sukuriamas naujas failas ir paliekamas originalas;
- Galima sukurti vienkartinį slaptažodį su užuomina, kuri būtų suprantama klientui.

2.9. Nuotolinio prisijungimo prie įmonės tinklo saugumo gerinimas

Viena iš pagrindinių priežasčių, kodėl buvo parengtas ir priimtas Reglamentas, yra užtikrinti asmens duomenų apsaugą. Reglamento 32 straipsnio 1 dalis numato, kad *Atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį [...] duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas [...]*. [7] Šios dalies b punktas taip pat nurodo, kad duomenų valdytojas privalo *[...] užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą.“* [7] Šių reikalavimų įgyvendinimui yra labai svarbu užtikrinti, kad prieiga prie įmonės serveriuose esančios informacijos būtų suteikiama tik įmonės darbuotojams.

Šiuo metu įmonėje yra naudojamas standartinis prisijungimas prie sistemos: kiekvienam darbuotojui sukuriamas unikalus prisijungimo vardas bei slaptažodis. Jie naudojami prisijungti prie įmonės ofise esančių kompiuterių. Šie kompiuteriai yra prijungti prie įmonės pagrindinio duomenų serverio. Nuotoliniam prisijungimui naudojama nuotolinio prisijungimo programa Tight VNC Viewer, kurią įdiegus darbuotojo asmeniniame kompiuteryje, jis gali prisijungti prie įmonės ofise esančių kompiuterių. Saugumo prasme šis metodas yra tinkamas, tačiau įmonė naudoją vieną slaptažodį visiems darbuotojams. Tokiu būdu gerokai susilpninamas visos sistemos saugumas.

Tarptautiniame informacinių technologijų standarto ISO 27040 B priede pateikiamos svarbiausios pagalbinės priemonės duomenų saugyklų saugumui užtikrinti. Kaip viena iš priemonių yra autentifikavimo stiprinimas. Tam turi būti naudojami:

- Stiprūs slaptažodžiai;
- Dviejų faktorių autentifikavimas. [12]

Kitame poskyryje apžvelgiamos dviejų faktorių autentifikavimo programos, kurios būtų taikomos nuotoliniam prisijungimui įmonėje. Kadangi bandomosios versijos nėra laisvai prieinamos, apžvalga daroma naudojantis programų kūrėjų pateikta informacija.

2.9.1. Dviejų faktorių autentifikavimo sprendimų palyginimas

Dviejų faktorių autentifikacija yra papildomas prisijungimo prie sistemų apsaugos lygis, užtikrinantis, kad prie sistemos nebus galima prisijungti net sužinojus darbuotojo vartotojo vardą bei slaptažodį. Tam yra naudojamos specialios programos. Toliau palyginamos dviejų pasaulyje garsių skaitmeninės saugos kompanijų – ESET ir SecurEnvoy dvigubo autentifikavimo produktus.

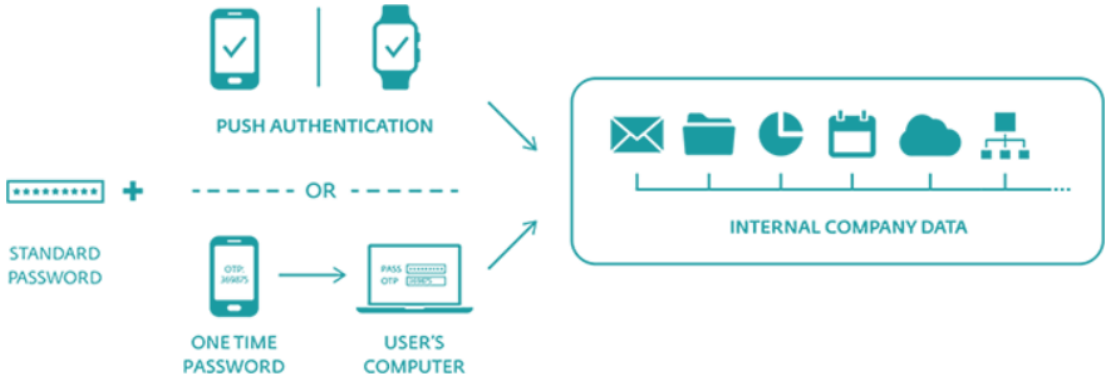
ESET Secure Autentication sprendimas suteikia galimybę pritaikyti dvigubo autentifikavimo prisijungimą prie dažniausiai naudojamų sistemų, tokių kaip VPN, Remote Desktop, Office 365, Outlook Web Access, VMware Horizon bei prisijungimui prie operacinių sistemų. Pagrindiniai gamintojo įvardijami ESET Secure Autentication privalumai yra šie:

- ESET Secure Authentication naudoja savo nuotolinio valdymo konsolę, kuri yra prieinama jungiantis per interneto naršyklę. Integruoti galima naudojantis *Active Directory*, kuris palengvina diegimo ir nustatymų procesą. Įdiegus sprendimą juo galima naudotis iškart, nereikalingi papildomi mokymai darbuotojams bei papildomi specialistai sprendimo diegimui;
- Sprendimas sukurtas taip, kad įmonės neturinčios IT skyriaus, galėtų jį įsidiegti savarankiškai, be papildomos pagalbos;

- Vienu metu veikia keliuose skirtinguose taškuose ir aptarnauja daug vartotojų;
- Nereikalinga papildoma įranga – veikia įdiegus specialią aplikaciją serveryje prie kurio norima jungtis;
- Platus vienkartinio slaptažodžio generavimo būdų pasirinkimas: aktyvintieji pranešimai (angl. *push notifications*), mobilioji programėlė, SMS bei pritaikytieji įrenginiai. [3]

Sprendimas palaiko šiuos VPN tinklus: Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet FortiGate, Juniper, Palo Alto, SonicWall.

Standartinė ESET Secure Autentication veikimo schema pavaizduota 2.22 pav.



2.22 pav. *Standartinė ESET Secure Autentication veikimo schema [3]*

Prisijungimo patvirtinimui naudojama mobilioji programėlė suteikia galimybę patvirtinti prisijungimą naudojant aktyvintus pranešimus (angl. *push notifications*) arba sugeneruojant vienkartinį slaptažodį, kurį reikia įvesti kompiuterio ekrane kartu su prisijungimo vardu ir pagrindiniu slaptažodžiu. Taip pat yra galimybė patvirtinti prisijungimą su išmaniuoju telefonu susietame išmaniajame laikrodyje. Vartotojo konfigūracija atliekama naudojant sistemos sugeneruotą ir su vartotojo paskyra susietą QR kodą, todėl tai gali atlikti pats vartotojas. Nėra poreikio kiekvieno darbuotojo telefone IT specialistui atlikti konfigūracijos.

SecurEnvoy SecurAccess kaip ir ESET kompanijos produktas yra skirtas įgyvendinti dvigubo autentifikavimo galimybę darbuotojams prisijungiant prie įmonės sistemos nuotoliniu būdu. SecurAccess sprendimas tinka tokioms sistemoms kaip Office 365, Microsoft Azure, VM Ware Horizon, Remote desktop bei VPN.

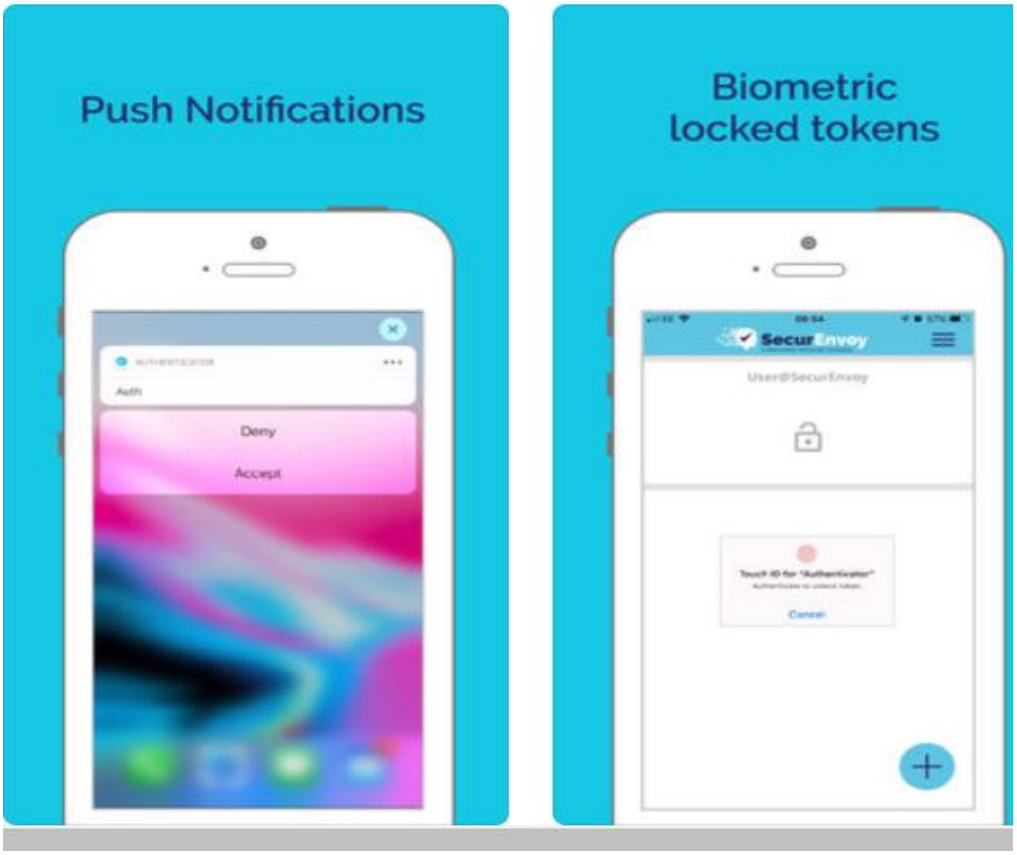
Pagrindiniai gamintojo įvardijami SecurAccess privalumai yra tokie:

- Visiems populiariausiems išmaniesiems telefonams pritaikyta mobilioji programėlė;
- Didelis vienkartinio slaptažodžio gavimo būdų pasirinkimas:
    - Mobiliuoju telefonu – vienkartinis SMS, SMS kodas, galiojantis visą dieną, balso skambutis bei aktyvintieji pranešimai;
    - Balso skambutis į fiksuoto ryšio telefoną vartotojams, kurie neturi prieigos prie išmaniųjų įrenginių;
    - Esant poreikiui vienkartinis slaptažodis gali būti siunčiamas automatiškai į vartotojo elektroninį paštą, tačiau šis būdas nėra rekomenduojamas dėl galimybės perimti elektroniniu paštu siunčiamus pranešimus.
- Nereikalingi papildomi slaptažodžių generatoriai;
- Pasirinkus slaptažodžio siuntimą SMS žinute, senos žinutės yra perrašomos, taip eliminuojant poreikį vartotojui trinti senas žinutes;
- Galimybė prijungti visus įmonės darbuotojus vienu metu naudojant diegimo vedlį. [20]

Sprendimas palaiko šiuos VPN tinklus: CheckPoint NGX, Cisco, Fortinet, Palo Alto, Pulse Secure bei Sonicwall NSV.

Tam, kad mažos įmonės neturinčios atskirų IT departamentų, galėtų pačios įsidiegti šį dvigubo prisijungimo sprendimą, gamintojas pateikia išsamius diegimo vadovus tiek programos diegimui serveryje, tiek darbuotojų kompiuteriuose bei mobiliuosiuose telefonuose.

Populiariausiam prisijungimui išmaniuoju telefonu skirta mobilioji programėlė palaiko galimybę patvirtinti prisijungimą aktyvintu pranešimu, sugeneruotu vienkartiniu slaptažodžiu bei naudojant biometrinius vartotojo duomenis – veido atpažinimą ir piršto antspaudą (2.23 pav.). Kaip ir ESET gamintojo mobiliojoje programėlėje, vartotojo konfigūracija atliekama naudojant sistemos sugeneruotą ir su vartotojo paskyra susietą QR kodą.



2.23 pav. *Prisijungimo patvirtinimas SecurAccess mobiliojoje programėlėje [20]*

Įvertinus gamintojų pateiktus šių dvigubo prisijungimo sprendimų duomenis, matoma, kad abu sprendimai yra labai panašūs savo funkcionalumu, todėl SecurEnvoy sprendimo pasirinkimą lemia tai, kad:

- Įmonėje neturint jokio VPN tinklo, SecurEnvoy gamintojo sprendimas suteikia platesnį palaikomų VPN tinklų pasirinkimą;
- SecureEnvoy sprendime yra daugiau prisijungimo patvirtinimo būdų;
- Mobilioji programėlė leidžia patvirtinti prisijungimą moderniausiu ir paprasčiausiu biometrinių vartotojo duomenų atpažinimo būdu.

2.10. Pranešimas apie duomenų apsaugos pažeidimą

Nepaisant visų dedamų pastangų užtikrinti asmens duomenų saugumą, gali įvykti nenumatyti duomenų saugos pažeidimai. Pagal Reglamento 33 ir 34 straipsnį, nustačius pažeidimo faktą, duomenų valdytojas yra įpareigotas pranešti apie tai priežiūros institucijai ir duomenų subjektui, šiuo atveju – klientui. Pagal Valstybinės duomenų apsaugos inspekcijos (toliau – VDAI) 2018 metų rekomendaciją dėl asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos saugumo incidentas yra apibrėžiamas taip:

Asmens duomenų saugumo pažeidimas – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami, persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga [15].

Galimi pažeidimo tipai pagal VDAI yra šie:

- Konfidencialumo pažeidimas – kai be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;
- Prieinamumo pažeidimas – kai netyčia arba neteisėtai prarandama prieiga prie duomenų arba jie yra sunaikinami;
- Vientisumo pažeidimas – kai asmens duomenys pakeičiami be leidimo arba netyčia. [15]

2.24 pav. pateikiamas pranešimo apie duomenų apsaugos pažeidimą procesas.

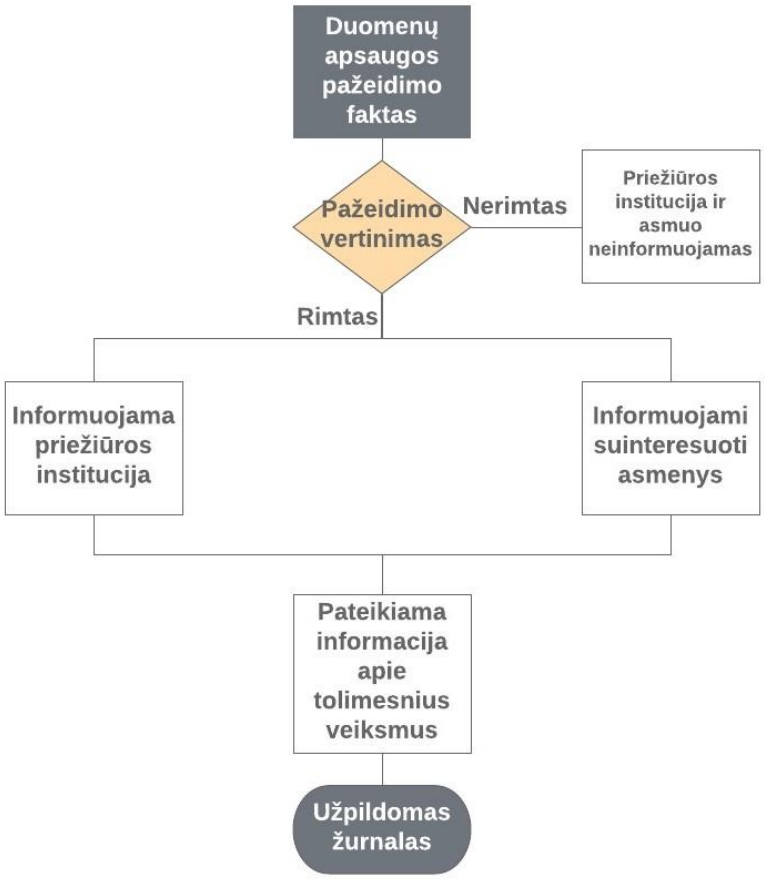
Suinteresuotam asmeniui pranešus apie duomenų apsaugos pažeidimo faktą, įmonės direktorius, atsakingas už duomenų apsaugos priežiūrą, įvertina galimą pavojų duomenų subjektų teisėms. Vertinant riziką yra vadovaujamasi šiais kriterijais:

- Pažeidimo tipą;
- Asmens duomenų pobūdį, apimtis (pvz., specialių kategorijų asmens duomenys);
- Kaip lengvai identifikuojamas fizinis asmuo;
- Pasekmių rimtumą fiziniams asmenims;
- Specialias fizinio asmens savybes (pvz., duomenys susiję su vaikais ar kitais pažeidžiamais asmenimis);
- Nukentėjusiųjų fizinių asmenų skaičių;
- Specialias duomenų valdytojo savybes (pvz., veiklos pobūdį). [15]

Nustačius, kad pažeidimas gali sukelti pavojų duomenų subjektams, yra informuojami asmenys, kurių asmens duomenims gali kilti pavojus, ir priežiūros institucija – šiuo atveju VDAI. Kadangi įmonė atlieka darbus tik Lietuvos teritorijoje, informuoti kitų šalių priežiūros institucijų nėra būtinybės. Jeigu nustatoma, kad pavojus duomenų subjektų teisėms nekyla, priežiūros institucija ir suinteresuoti asmenys neinformuojami.

Informuojant VDAI minimaliai turi būti pateikiama ši informacija [7]:

- Asmens duomenų saugumo pažeidimo pobūdis bei galimai paveiktų subjektų apytikslis skaičius;
- Už duomenų apsaugos užtikrinimą įmonėje atsakingo asmens kontaktai tam, kad būtų galima susisiekti, jeigu reikės daugiau informacijos;
- Tikėtinos asmens duomenų saugumo pažeidimo pasekmės;
- Priemonės, kurių ėmėsi arba ketina imtis įmonė, kad būtų pašalintas pažeidimas.



2.24 pav. *Pranešimo apie duomenų apsaugos pažeidimą procesas*

Informuojant apie pažeidimą duomenų subjektus, turi būti pateikta tokia pati informacija, kaip ir VDAI, tik nereikia pranešti apie pažeidimo pobūdį ir paveiktų asmenų skaičių.

Pranešus suinteresuotiems asmenims ir priežiūros institucijai, yra užpildomas įmonės žurnalas tam, kad reikalui esant būtų galima pateikti detalesnę informaciją priežiūros institucijai. Įvertinus priežastis, dėl kurių atsirado saugumo pažeidimas bei jo pasekmes, yra nusprendžiama, kokių priemonių bus imtasi ateityje, kad būtų užkirstas kelias panašiems incidentams.

2.11. Apibendrinimas

Šiame skyriuje įvertinta esama įmonės duomenų apsaugos situacija bei nustatyti jos veiklos procesai, neatitinkantys Reglamento reikalavimų. Aprašyti duomenų perkėlimo, sunaikinimo procesai bei nustatyta tvarka, kurios turi būti laikomasi informuojant priežiūros instituciją bei suinteresuotus asmenis įvykus asmens duomenų saugumo pažeidimui.

Atlikus populiariausių duomenų šifravimo, vaizdų redagavimo, bei nuotolinio prisijungimo saugumą stiprinančio dvigubo autentifikavimo technologinių sprendimų palyginimą, pateikti pasiūlymai, kuriuos iš jų įmonė turėtu naudoti siekdama optimalaus santykio tarp duomenų apsaugos reikalavimų įgyvendinimo, bei įmonės veiklos našumo.

Išvados

1. Atlikus duomenų apsaugą reglamentuojančių teisės aktų analizę nustatyta, kad asmens duomenų sąvoka ES teisės aktuose įtvirtinta 1950 m. priimtoje Europos žmogaus teisių konvencijoje, o šiuo metu asmens duomenų apsaugą reglamentuoja Bendrasis duomenų apsaugos reglamentas ir su juo suderinti nacionalinės teisės aktai. Palyginus asmeninių duomenų apsaugos sampratą ES ir JAV, galima teigti, kad ES įmonės, vykdančios veiklą JAV, susiduria su mažesniu teisiniu reguliavimu nei JAV įmonės Europoje, nes ES asmens duomenims yra priskiriama akivaizdžiai daugiau asmeninės informacijos nei Jungtinėse Valstijose.

2. Įvertinus esamą duomenų apsaugos srities situaciją tiriamoje įmonėje, nustatyta, kad įmonėje asmens duomenų apsaugai nėra skiriamas pakankamas dėmesys, nes atliekant geodezinius matavimus surenkama daug perteklinės informacijos, kurios laikymo ir naudojimo sąlygos sudaro prielaidą atsirasti duomenų apsaugos pažeidimams.

3. Nustačius įmonės veikloje surenkamus asmens duomenis bei jų naudojimo specifiką, identifikuotos BDAR taikymo sritys, kuriose įmonės procesai neatitinka keliamų saugumo reikalavimų. Dėl ribotos darbo apimties tolesniam nagrinėjimui buvo pasirinktos tik tos veiklos sritys, kurios yra tiesiogiai susijusios su geodezine veikla, ir jose renkami bei apdorojami asmens duomenys.

4. Įvertinus darbe pateiktą informaciją apie įmonės veiklą ir Reglamento reikalavimus, sumodeliuoti ir aprašyti procesai, skirti pertekliniams duomenims maskuoti, asmens duomenims perkelti bei ištrinti ir informuoti priežiūros institucijas apie duomenų saugumo pažeidimą įmonėje, nes nustatyta, kad šiuo metu įmonėje naudojami procesai nepakankamai užtikrina asmens duomenų saugumą. Taip pat parinktos nuotolinio prisijungimo technologijos, stiprinančios nuotolinio prisijungimo saugumą, nes šiuo metu naudojamas būdas suteikia prielaidas asmens duomenų nutekinimui ar praradimui.

Rekomendacijos

Išanalizavus BDAR reikalavimus ir atlikus populiariausių vaizdų redagavimo, duomenų šifravimo bei dvigubo autentifikavimo sprendimų palyginimą, pateikiamos šios rekomendacijos:

1. Pertekliniams duomenims panoraminėse nuotraukose maskuoti, siūloma naudoti atviro kodo vaizdų redagavimo programinę įrangą PhotoScape X, suteikiančią galimybę neprarandant nuotraukų kokybės ir su minimaliu žingsnių skaičiumi redaguoti didelį kiekį nuotraukų, maksimaliai neišnaudojant kompiuterio resursų.

2. Įvertinus įmonės dydį ir vykdomą veiklą, siūloma nesteigti duomenų apsaugos pareigūno pareigybės, o visas pareigas, susijusias su asmens duomenų apsauga, pavesti vykdyti įmonės direktoriui.

3. Perduodant duomenis kitam vykdytojui, užtikrinti duomenų saugumą siūloma naudoti duomenų šifravimo įrankį Secure IT, kuriuo užšifruoti failai gali būti iššifruoti naudojant standartinį kompiuterio operacinėje sistemoje esantį dešifravimo įrankį, su vienkartiniu tik klientui ir įmonei žinomu slaptažodžiu bei tinkantį negrįžtamai sunaikinti failus.

4. Šiuo metu naudojamą nuotolinio prisijungimo būdą pakeisti saugiu VPN tinklu, o prisijungimui stiprinti siūloma naudoti SecurEnvoy dvigubo autentifikavimo sprendimą, suteikiantį didesnį palaikomų VPN tinklų pasirinkimą ir platesnį prisijungimo patvirtinimo būdų pasirinkimą, įskaitant moderniausią – biometrinių duomenų atpažinimą.

Literatūros sąrašas

1. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 28/01/1981. European Treaty Series - No. 108.
2. Convention for the Protection of Human Rights and Fundamental Freedoms. Rome, 4.XI.1950
3. ESET SECURE AUTHENTICATION [interaktyvus] 2019. ESET. [Žiūrėta 2019 m. balandžio 29 d.]. Prieiga per internetą: <https://www.eset.com/lt/verslui/endpoint-apsauga/two-factor-authentication/>
4. 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių). Europos Sąjungos oficialusis leidinys L201, paskelbta 2002 m. liepos 31 d.
5. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR. Europos Sąjungos oficialusis leidinys L119, paskelbta 2016 m. gegužės 4 d.
6. 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo. Europos Sąjungos oficialusis leidinys L8, paskelbta 2001 m. sausio 12 d.
7. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). Europos Sąjungos oficialusis leidinys L119, paskelbta 2016 m. gegužės 4 d.
8. Europos Sąjungos Pagrindinių Teisių Chartija (2012/C 326/02)
9. GIMP 2.0: GNU IMAGE MANIPULATION PROGRAM [interaktyvus] 2019. Gimp. [Žiūrėta 2019 m. sausio 26 d.]. Prieiga per internetą: <https://www.gimp.org/>
10. Google Street view [inteaktyvus] 2019. Google Inc. [Žiūrėta 2019 m. balandžio 30 d.]. Prieiga per internetą: <https://www.google.lt/maps/@51.7307059,-0.3036106,3a,75y,112.83h,90.32t/data=!3m6!1e1!3m4!1srbMUTSRfuK_HWnFyV56_5A!2e0!7i13312!8i6656?hl=en>
11. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo Nr. I-1374 pakeitimo įstatymas (Lietuvos Respublikos Seimas/Įstatymas/ XIII-1426/ 2018 06 30/TAR, 2018-07-11, Nr. 11733)

12. LST EN ISO/IEC 27040:2016 Informacinės technologijos. Saugumo metodai. Saugojimo saugumas (tapatus ISO/IEC 27040:2015), Vilnius, 2016. 113p.
13. PhotoScape X. Fun and Easy Photo Editor [interaktyvus] 2019. MOOII TECH. [Žiūrėta 2019 m. sausio 25 d.]. Prieiga per internetą: <http://x.photoscape.org/>
14. Photoshop CC [interaktyvus] 2019. Adobe. [Žiūrėta 2019 m. sausio 25 d.]. Prieiga per internetą: <https://www.adobe.com/lt/creativecloud/plans.html?single_app=photoshop>
15. Rekomendacija dėl asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos (2018 m.) [interaktyvus] 2018. Valstybinė duomenų apsaugos inspekcija. [Žiūrėta 2019 m. gegužės 4 d.]. Prieiga per internetą: <https://www.ada.lt/go.php/lit/Rekomendacija-del-asmens-duomenu-saugumo-pazeidimu-nustatymo-tyrimo-praneimo-apie-juos-ir-dokumentavimo-tvarkos-2018-m>
16. Rubinstein, I. 2013 Big Data: The End of Privacy or a New Beginning? New York University Public Law and Legal Theory Working Papers, Paper 357.
17. Secure IT File Encryption [interaktyvus] 2019. Cypherix. [Žiūrėta 2019 m. balandžio 27 d.]. Prieiga per internetą: <https://www.cypherix.com/secureit2000/>
18. SensiGuard [interaktyvus] 2019. WebMinds. [Žiūrėta 2019 m. balandžio 28 d.]. Prieiga per internetą: <https://www.sensiguard.com/download>
19. Solove, D.J.; Schwartz, P.M. 2013 Reconciling Personal Information in the United States and European Union. GW Law Faculty Publications & Other Works Paper 956.
20. Trusted Multi-Factor Authentication Paired With Your Choice of Deployment Offers Security Without Compromise [interaktyvus] 2019. SecurEnvoy. [Žiūrėta 2019 m. balandžio 29 d.]. Prieiga per internetą: <https://www.securenvoy.com/en-us>
21. Zhao, H.; Dong, H.X. 2017 Research on Personal Privacy Protection of China in the Era of Big Data. Open Journal of Social Sciences , 5: 139-145.
22. 7-Zip file archiver [interaktyvus] 2019. Igor Pavlov. [Žiūrėta 2019 m. balandžio 28 d.]. Prieiga per internetą: <https://www.7-zip.org>

Priedai

A priedas. UAB „LiMAP“ pažyma.

LiMAP

Life in MAP

Vilniaus Gedimino Technikos Universiteto
Fundamentinių mokslų fakulteto
Informacinių technologijų katedros vedėjui

2018 gegužės 07 d. Nr. LIM-18-ID-030

PAŽYMA

Pažymime, kad Martyno Valauskio parengtas darbas, tema „Bendrojo duomenų apsaugos reglamento įgyvendinimo geodezinių paslaugų įmonėje galimybių studija“ yra aktualus įmonės veiklos tobulinimui ir bus tuo tikslu panaudotas.

Direktorius Andrius Aponas

LIETUVOS RESPUBLIKA * REPUBLIC OF LITHUANIA * VILNIUS *
LIMAP, UAB
Ltd.

Adresas Šaltinėkio g. 15-712, Vilnius
Įmonės k. 304 225 378
PVM mok.k. LT 1000 1018 4513

A/s LT55 4010 0510 0368 8122
Bankas AB DNB Bankas
Reg.tvarkyt. VĮ „Reg. centras“ Vilniaus filialas

El.paštas info@limap.lt
El.svetė www.limap.lt
Tel. nr. 370 (647) 57535

B priedas. Matavimo darbų atlikimo sutarties pavyzdys.