MARIJAMPOLĖS KOLEGIJA
(Kodas 211967140)

PATVIRTINTA
Marijampolės kolegijos direktoriaus
2020 m. liepos 7 d. įsakymu Nr. 1V-74

ASMENS DUOMENŲ TVARKYMO TAISYKLĖS

2020

Turinys

Contents

I SKYRIUS 4

BENDROSIOS NUOSTATOS 4

II SKYRIUS 8

PAGRINDINIAI ASMENS DUOMENŲ TVARKYMO PRINCIPAI 8

III SKYRIUS 9

ASMENS DUOMENŲ TVARKYMO TEISINIAI PAGRINDAI 9

IV SKYRIUS 10

ASMENS DUOMENŲ TVARKYMO TIKSLAI, SAUGOJIMO TERMINAI IR DUOMENŲ TEIKIMAS TRETIESIEMS ASMENIMS 10

V SKYRIUS 12

DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI 12

VI SKYRIUS 13

VAIZDO DUOMENŲ TVARKYMAS 13

VII SKYRIUS 15

REIKALAVIMAI DARBUOTOJAMS, TVARKANTIEMS ASMENS DUOMENIS IR JŲ ATSAKOMYBĖ 15

VIII SKYRIUS 16

TECHNINĖS IR ORGANIZACINĖS DUOMENŲ SAUGUMO PRIEMONĖS 16

IX SKYRIUS 19

ASMENS DUOMENŲ TVARKYMUI TAIKOMŲ SAUGUMO PRIEMONIŲ SĄRAŠAS 19

X SKYRIUS 21

ASMENS DUOMENŲ TVARKYTOJAI IR GAVĖJAI 21

XI SKYRIUS 22

DUOMENŲ SUBJEKTŲ TEISĖS IR JŲ ĮGYVENDINIMO TVARKA 22

XII SKYRIUS 26

POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS (PDAV) IR IŠANKSTINĖS KONSULTACIJOS SU PRIEŽIŪROS INSTITUCIJA 26

XIII SKYRIUS 27

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMAS 27

XIV SKYRIUS 30

ASMENS DUOMENŲ APSAUGOS PAREIGŪNAS 30

BAIGIAMOSIOS NUOSTATOS 31

1 Priedas. **MARIJAMPOLĖS KOLEGIJOS ASMENS DUOMENŲ TVARKYMO REGISTRAVIMO ŽURNALAS** 32

2 Priedas. **PRAŠYMASDĖL DUOMENŲ SUBJEKTO TEISIŲ (-ĖS) ĮGYVENDINIMO** 33

3 Priedas. **PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ** 35

4 Priedas. **ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMO ATASKAITA** 37

5 Priedas. **PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ** 42

6 Priedas. **ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMO ŽURNALAS** 48

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Asmens duomenų tvarkymo taisyklių (toliau – Taisyklės) tikslas	reglamentuoti asmenų, kurių duomenis tvarko Marijampolės kolegija (toliau – Kolegija), asmens duomenų tikslus, nustatyti duomenų subjektų teises ir jų įgyvendinimo tvarką, įtvirtinti organizacines ir technines duomenų apsaugos priemones, reguliuoti asmens duomenų tvarkytojo pasitelkimo atvejus bei užtikrinti Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (toliau – ADTAĮ), Bendrojo duomenų apsaugos reglamento (ES) 2016/679 (toliau – BDAR), kitų teisės aktų, reglamentuojančių asmens duomenų tvarkymą ir apsaugą, laikymąsi ir įgyvendinimą.
2. Pagrindinės taisyklėse vartojamos sąvokos:	
Sąvoka	**Apibrėžimas**
Asmens duomenys	bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (**duomenų subjektas)** tiesiogiai arba netiesiogiai, visų pirma pagal identifikatorių, pavyzdžiui vardą ir pavardę, asmens kodą, buvimo vietos duomenis arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius. Pavyzdžiui: vaizdo įrašas, garso įrašas, pirkinių istorija, naršymo svetainėje statistika, lojalumo kortelės numeris ir pan.
Duomenų subjektas	fizinis asmuo, kurio asmens duomenis tvarko duomenų valdytojas ar duomenų tvarkytojas. Pavyzdžiui: darbuotojas, klientas, vartotojas, gyventojas ir pan.
Asmens duomenų tvarkymas (toliau – duomenų tvarkymas)	bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, pavyzdžiui rinkimas, įrašymas, rūšiavimas, kaupimas, klasifikavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas.
Duomenų valdytojas	fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones.
Duomenų tvarkytojas	fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis. Pavyzdžiui: personalo apskaitos sistemos tiekėjas, informacinių technologijų, serverio, interneto parduotuvės sistemos ar talpinimo paslaugos tiekėjas ir pan.
Duomenų valdytojas (toliau – Kolegija)	**Marijampolės kolegija, 211967140, Marijampolės sav. Marijampolės m. P. Armino g. 92-4.**
Duomenų gavėjas	fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuriai atskleidžiami asmens duomenys, nesvarbu, ar tai trečioji šalis, ar ne. Valdžios institucijos, kurios pagal valstybės narės teisės aktus gali gauti asmens duomenis vykdydamos konkretų tyrimą, nelaikomos duomenų gavėjais; tvarkydamos tuos

	duomenis tos valdžios institucijos laikosi taikomų duomenų tvarkymo tikslus atitinkančių duomenų apsaugos taisyklių.
Trečioji šalis	fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri nėra duomenų subjektas, duomenų valdytojas, duomenų tvarkytojas, arba asmenys, kuriems tiesioginiu duomenų valdytojo ar duomenų tvarkytojo įgaliojimu leidžiama tvarkyti asmens duomenis. Pavyzdžiui: partneriai, tiekėjai, nuomotojai, Valstybinė mokesčių inspekcija, bankai ir pan.
Specialių kategorijų asmens duomenys	asmens duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, taip pat genetiniai duomenys, biometriniai duomenys, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenys (asmens duomenys, susiję su fizine ar psichine fizinio asmens sveikata, įskaitant duomenis apie sveikatos priežiūros paslaugų teikimą, atskleidžiantys informaciją apie to fizinio asmens sveikatos būklę) arba duomenys apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją.
Duomenų apsaugos pareigūnas (toliau – Pareigūnas)	Kolegijos vadovo paskirtas darbuotojas ar paslaugų teikėjas, atliekantis BDAR nustatytas duomenų apsaugos pareigūno funkcijas.
Duomenų subjekto sutikimas	bet koks laisva valia duotas, konkretus ir nedviprasmiškas tinkamai informuoto duomenų subjekto valios išreiškimas pareiškimu arba vienareikšmiais veiksmais kuriais jis sutinka, kad būtų tvarkomi su juo susiję asmens duomenys.
Įgalioti tvarkyti asmens duomenis darbuotojai	duomenų valdytojo darbuotojai (t. y. asmenys tarp kurių ir duomenų valdytojo yra sudarytos darbo sutartys) ir / arba kiti fiziniai asmenys, kurie sutarčių ar kitu pagrindu turi teisę tvarkyti duomenų valdytojo tvarkomus asmens duomenis.
Vaizdo stebėjimas	vaizdo duomenų, susijusių su fiziniu asmeniu, tvarkymas naudojant automatizuotas vaizdo stebėjimo priemones (vaizdo ir fotokameras ar pan.), nepaisant to, ar šie duomenys yra išsaugomi laikmenoje.
Vaizdo įrašas	vaizdo stebėjimo kameromis užfiksuoti ir vaizdo duomenų įrašymo įrenginiuose išsaugoti vaizdo duomenys.
Prieiga prie vaizdo įrangos	fizinė prieiga ar prieiga elektroninio ryšio priemonėmis, suteikianti asmeniui galimybę keisti, šalinti ar atnaujinti techninės vaizdo įrangos komponentes ar programinę įrangą, nustatyti vaizdo įrangos veikimo parametrus.
Interneto svetainė	Kolegijos svetainė, kurioje yra pristatoma Kolegijos veikla.
Profiliavimas	bet kokios formos automatizuotas Asmens duomenų tvarkymas, kai Asmens duomenys naudojami siekiant įvertinti tam tikrus su fiziniu asmeniu susijusius asmeninius aspektus, visų pirma siekiant išanalizuoti ar numatyti aspektus, susijusius su to fizinio asmens darbo rezultatais, ekonomine situacija, sveikatos būkle, asmeniniais pomėgiais, interesais, patikimumu, elgesiu, buvimo vieta arba judėjimu.
Techninės ir organizacinės saugumo priemonės	tai priemonės, kuriomis siekiama apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo ar netyčinio praradimo, pakeitimo, neteisėto atskleidimo ar prieigos, ypač tais atvejais, kai tvarkymas susijęs su duomenų perdavimu tinkle, ir visos kitos neteisėtos tvarkymo formos.
Duomenų bazė	yra organizuotas (susistemintas, metodiškai sutvarkytas) duomenų

	rinkinys, kuriuo galima individualiai naudotis elektroniniu ar kitu būdu.
Neatitiktis	bet koks įvykis, turėjęs ar galintis turėti įtakos asmens duomenų saugumui.
Informacijos saugumo įvykis	nustatytas sistemos, tarnybos ar tinklo įvykis, rodantis, kad yra galima saugumo užtikrinimo spraga ar apsaugos priemonių trikdis arba anksčiau nenumatyta situacija, kuri gali būti svarbi saugumui.
Informacijos saugumo incidentas	vienas ar daugiau nepageidaujamų ir netikėtų informacijos saugumo įvykių, turinčių didelę tikimybę pakenkti veiklai ir keliančių grėsmę informacijos saugumui.
Asmens duomenų tvarkymo registravimo žurnalas	Kolegijos įgalioto (-ų) darbuotojo (-ų) pildomas žurnalas, skirtas Kolegijoje pateiktų prašymų, susijusių su asmens duomenų tvarkymu registracijai ir administravimui. Duomenų subjektų prašymus dėl tvarkomų asmens duomenų priima ir Kolegijos Asmens duomenų tvarkymo registravimo žurnale (Taisyklių priedas Nr. 1) užregistruoja Pareigūnas arba Kolegijos vadovo įgaliotas darbuotojas.
Korekcinis veiksmas	veiksmas, atliekamas siekiant pašalinti nustatytos neatitikties ar kitos nepageidaujamos situacijos priežastį.
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.
Duomenų tvarkymo veiklos įrašas (toliau – DTVĮ)	Dokumentas, kuriame fiksuojama Kolegijos vykdomų duomenų tvarkymo veiklų tikslai, duomenų subjektai, duomenų gavėjai, duomenų ištrynimo terminai ir kita reikalaujama arba reikšminga informacija apie duomenų tvarkymo veiklas.
Priežiūros institucija	Valstybinė duomenų apsaugos inspekcija (toliau – VDAI).
3. Kitos, aukščiau nenurodytos Taisyklėse vartojamos sąvokos atitinka ADTAĮ ir BDAR vartojamas sąvokas.	
4. Taisyklės taikomos tvarkant fizinių asmenų duomenis tiek automatiniu būdu, tiek neautomatiniu būdu tvarkant asmens duomenų susistemintas rinkmenas: klientų sąrašus, kartotekas, bylas, sąvadus ir kita.	
5. Taisyklės privalomos visiems Kolegijoje pagal darbo sutartis dirbantiems darbuotojams (toliau – Darbuotojai), kurie yra įgalioti tvarkyti Kolegijoje esančius asmens duomenis arba eidami savo pareigas juos sužino, bei kitiems sutartiniais pagrindais paslaugas teikiantiems asmenims, kurie gali tvarkyti arba sužino asmens duomenis.	
6. Duomenų valdytojas turi šias teises:	6.1. rengti ir priimti vidinius teisės aktus, reglamentuojančius duomenų tvarkymą; 6.2. spręsti dėl tvarkomų asmens duomenų teikimo; 6.3. paskirti už asmens duomenų apsaugą atsakingus asmenis; 6.4. įgalioti duomenų tvarkytojus tvarkyti asmens duomenis; 6.5. kitas teisės aktuose nustatytas teises.
7. Duomenų valdytojas turi šias pareigas:	7.1. užtikrinti ADTAĮ ir kituose teisės aktuose, reglamentuojančiose asmens duomenų tvarkymą, nustatytų asmens duomenų tvarkymo reikalavimų laikymąsi; 7.2. įgyvendinti duomenų subjekto teises ADTAĮ ir šiose Taisyklėse nustatyta tvarka; 7.3. užtikrinti asmens duomenų saugumą, įgyvendinant tinkamas organizacines ir technines asmens duomenų saugumo priemones;

	7.4. parinkti tik tokį duomenų tvarkytoją, kuris garantuotų reikiamas technines ir organizacines asmens duomenų apsaugos priemones ir užtikrintų, kad tokių priemonių būtų laikomasi; 7.5. teisės aktų nustatytais atvejais paskirti duomenų apsaugos pareigūną; 7.6. teisės aktų nustatytais atvejais pildyti duomenų tvarkymo veiklos įrašus; 7.7. teisės aktų nustatytais atvejais atlikti poveikio duomenų apsaugai vertinimą; 7.8. valdyti asmens duomenų saugumo pažeidimus ir teisės aktuose nustatytais atvejais pranešti apie juos priežiūros institucijai ir duomenų subjektams; 7.9. kitas teisės aktuose nustatytas pareigas.
8. Duomenų valdytojas atlieka šias funkcijas:	8.1. nustato duomenų tvarkymo tikslus ir priemones; 8.2. organizuoja duomenų tvarkymą; 8.3. analizuoja technologines, metodologines ir organizacines duomenų tvarkymo problemas ir priima sprendimus, reikalingus tinkamam duomenų tvarkymui užtikrinti; 8.4. teikia metodinę pagalbą darbuotojams duomenų tvarkymo klausimais; 8.5. organizuoja darbuotojų mokymus asmens duomenų teisinės apsaugos klausimais; 8.6. užtikrina duomenų subjekto teisių įgyvendinimą; 8.7. kitas teisės aktuose nustatytas funkcijas.

II SKYRIUS
PAGRINDINIAI ASMENS DUOMENŲ TVARKYMO PRINCIPAI

1. Kolegijoje asmens duomenys tvarkomi laikantis šių asmens duomenų tvarkymo ir apsaugos principų	1.1. Asmens duomenis tvarkyti teisėtai, sąžiningai ir skaidriai **(teisėtumo, sąžiningumo ir skaidrumo principas)**; 1.2. Asmens duomenis rinkti nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkyti tikslais, nesuderinamais su nustatytaisiais prieš renkant asmens duomenis **(tikslo apribojimo principas)**; Tolesnis duomenų tvarkymas archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais nėra laikomas nesuderinamu su pirminiais tikslais. Kolegijos darbuotojai turi teisę rinkti, tvarkyti, perduoti, saugoti, naikinti ar kitaip naudoti asmens duomenis tik atlikdami savo tiesiogines funkcijas, apibrėžtas pareigybės aprašyme ar kitame Kolegijos lokaliniame teisės akte arba Kolegijos vadovo pavedimu ir tik teisės aktų nustatyta tvarka. Kolegijos darbuotojams draudžiama savavališkai rinkti, tvarkyti, perduoti, saugoti, naikinti ar kitaip naudoti asmens duomenis; 1.3. Tvarkomi asmens duomenys turi būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi **(duomenų kiekio mažinimo principas)**; 1.4. Tvarkomi asmens duomenys turi būti tikslūs ir prireikus atnaujinami; turi būti imamasi visų pagrįstų priemonių užtikrinti, kad asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba ištaisomi **(tikslumo principas)**; 1.5. Tvarkomus asmens duomenis laikyti tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi; asmens duomenis galima saugoti ilgesnius laikotarpius, jeigu asmens duomenys bus tvarkomi tik archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais, įgyvendinus atitinkamas technines ir organizacines priemones, kurių reikalaujama BDAR siekiant apsaugoti duomenų subjekto teises ir laisves **(saugojimo trukmės apribojimo principas);** 1.6. Tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo **(vientisumo ir konfidencialumo principas)**; 1.7. Duomenų valdytojas yra atsakingas ir turi sugebėti įrodyti, kad yra laikomasi aukščiau nurodytų principų **(atskaitomybės principas)**.
2. Asmens duomenų tvarkymo principų laikymąsi užtikrina Kolegijos vadovas ir jo įgalioti darbuotojai, imdamiesi atitinkamų organizacinių priemonių (įsakymai, nurodymai, rekomendacijos, pavedimai ir pan.), kad būtų įgyvendintos Duomenų valdytojui priskirtos prievolės. Pavyzdžiui: įpareigoti nutraukti neteisėtus ar asmens duomenų apsaugos reikalavimus pažeidžiančius duomenų tvarkymo veiksmus, sunaikinti dokumentų, kuriuose yra nurodyti asmens duomenys, kopijas ir pan.).	

III SKYRIUS
ASMENS DUOMENŲ TVARKYMO TEISINIAI PAGRINDAI

1. Kolegija asmens duomenis tvarko tik esant bent vienam iš šių teisinių pagrindų:	1.1. Duomenų subjektas duoda sutikimą, kad jo asmens duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais (pavyzdžiui, Kolegijos interneto svetainėje duomenų subjektas užsisako naujienlaiškius pateikdamas savo el. pašto adresą); 1.2. Duomenų tvarkymas yra būtinas siekiant įvykdyti sutartį, kurios šalis yra duomenų subjektas, arba siekiant imtis veiksmų duomenų subjekto prašymu prieš sudarant sutartį; 1.3. Tvarkyti duomenis būtina, kad būtų įvykdyta duomenų valdytojui taikoma teisinė prievolė; 1.4. Tvarkyti duomenis būtina, siekiant apsaugoti duomenų subjekto ar kito asmens gyvybinius interesus (pavyzdžiui, Kolegija tvarko darbuotojo artimųjų kontaktinius duomenis, su kuriais galėtų susisiekti įvykus nelaimei ar ekstremaliam įvykiui); 1.5. Duomenų tvarkymas yra būtinas viešojo intereso labui arba vykdant pavestas viešosios valdžios funkcijas; 1.6. Tvarkyti duomenis būtina siekiant teisėtų duomenų valdytojo ar trečiosios šalies interesų, išskyrus atvejus, kai duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą, yra už šiuos duomenų valdytojo teisėtus interesus viršesni, ypač kai duomenų subjektas yra vaikas (pavyzdžiui, Kolegija vykdo vaizdo stebėjimą darbuotojų, kitų duomenų subjektų ir turto saugumo užtikrinimo tikslu.
2. Kolegija specialių kategorijų asmens duomenis tvarko tik esant bent vienam iš šių pagrindų:	2.1. Tvarkyti duomenis būtina, kad duomenų valdytojas arba duomenų subjektas galėtų įvykdyti prievoles ir naudotis specialiomis teisėmis darbo ir socialinės apsaugos teisės srityje, kiek tai leidžiama Europos Sąjungos arba valstybės narės teisėje arba pagal valstybės narės teisę sudaryta kolektyvine sutartimi, kuriuose nustatytos tinkamos duomenų subjekto pagrindinių teisių ir interesų apsaugos priemonės; 2.2. Tvarkyti duomenis būtina, kad būtų apsaugoti gyvybiniai duomenų subjekto arba kito fizinio asmens interesai, kai duomenų subjektas dėl fizinių ar teisinių priežasčių negali duoti sutikimo; 2.3. Tvarkomi asmens duomenys, kuriuos duomenų subjektas yra akivaizdžiai paskelbęs viešai; 2.4. Tvarkyti duomenis būtina siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus; 2.5. Tvarkyti duomenis būtina dėl svarbių viešojo intereso priežasčių, vadovaujantis Europos Sąjungos arba valstybės narės teise, kurie turi būti proporcingi tikslui, kurio siekiama, nepažeisti esminių teisės į duomenų apsaugą nuostatų; 2.6. Tvarkyti duomenis būtina profilaktinės arba darbo medicinos tikslais, siekiant įvertinti darbuotojo darbingumą; 2.7. Tvarkyti duomenis būtina dėl viešojo intereso priežasčių visuomenės sveikatos srityje, pavyzdžiui, siekiant apsisaugoti nuo rimtų tarpvalstybinio pobūdžio grėsmių sveikatai.

IV SKYRIUS
ASMENS DUOMENŲ TVARKYMO TIKSLAI, SAUGOJIMO TERMINAI IR DUOMENŲ TEIKIMAS TRETIESIEMS ASMENIMS

1. Asmens duomenys Kolegijoje tvarkomi šiais tikslais (įskaitant, bet neapsiribojant atvejais kai gaunamas atskiras duomenų subjekto sutikimas dėl duomenų tvarkymo):	1.1. Darbdavio teisinių prievolių vykdymas: darbo sutarčių sudarymas, tinkamas vykdymas, apskaita (darbo užmokesčio ir kitų išmokų administravimas) ir nutraukimas; Praktikos sutarčių sudarymas; Mokymai; Duomenų valdytojo kaip darbdavio pareigų, nustatytų teisės aktuose, tinkamas vykdymas; Tinkamos komunikacijos su darbuotojais ne darbo metu palaikymas; Tinkamų darbo sąlygų užtikrinimas (struktūros tvarkymas, esamų ir buvusių darbuotojų informacijos valdymas, dokumentų valdymas, turimų materialinių ir finansinių išteklių valdymas); 1.2. Kolegijos veiklos užtikrinimo ir tęstinumo vykdymas: sutarčių sudarymo bei vykdymo, pirkimų procedūrų organizavimas ir vykdymas; 1.3. Komunikacijai su duomenų subjektais (užklausų, komentarų ir nusiskundimų) administravimas; 1.4. Studijų proceso administravimas; 1.5. Kolegijoje besilankančių ir bendrabutyje gyvenančių asmenų bei jų turto saugumo užtikrinimas (vaizdo stebėjimas); 1.6. Kandidatų į darbo vietas gyvenimo aprašymų (CV) duomenų bazės administravimas; 1.7. Visuomenės informavimas apie Kolegijos veiklą, dalyvavimą parodose, konferencijose, pristatymuose ir kituose renginiuose.
2. Kiekvienu tikslu atskirai, Kolegijoje sudaromas DTVĮ, kuriame nurodomas duomenų saugojimo terminas, duomenų gavėjų kategorijos ir kita papildoma informacija.	
3. Asmens duomenys saugomi ne ilgiau, negu to reikalauja duomenų tvarkymo tikslai.	
4. Pasibaigus duomenų saugojimo terminui asmens duomenys yra visam laikui ištrinami, sunaikinami, išskyrus, jei teisės aktai nenumato kitaip. Asmens duomenų saugojimo terminai nustatyti Kolegijos vadovo patvirtintame dokumentacijos plane.	
5. Dėl asmens duomenų naikinimo dokumentuose, informacinėse sistemose ir duomenų bazėse, darbuotojai privalo kreiptis į Kolegijos vadovo įgaliotą darbuotoją.	
6. Sunaikinimas apibrėžiamas kaip fizinis ar techninis veiksmas, kuriuo duomenys padaromi neatkuriamais:	6.1. elektronine forma saugomi asmens duomenys sunaikinami juos ištrinant be galimybės atkurti; 6.2. popieriniai dokumentai, kuriuose yra asmens duomenų, susmulkinami, o likučiai saugiu būdu sunaikinami.
7. Jeigu duomenys naudojami kaip įrodymai civilinėje, administracinėje ar baudžiamojoje byloje ar kitais teisės aktų nustatytais atvejais, duomenys gali būti saugomi tiek, kiek reikalinga šiems duomenų tvarkymo tikslams pasiekti ir sunaikinami nedelsiant, kai tampa nebereikalingi.	
8. Asmens duomenų perdavimas Kolegijos viduje vyksta darbuotojams susirašinėjant darbo el. paštu, perduodant rašytinius dokumentus, naudojantis kitomis informacinėmis sistemomis.	
9. Kolegijos tvarkomus asmens duomenis, Kolegija gali perduoti tretiesiems asmenims vykdant teisės aktuose įtvirtintas Kolegijos pareigas, valstybės ir (ar) savivaldos institucijų nurodymus bei kitų teisės aktų nustatytais atvejais ir tvarka.	
10. Asmens duomenys Kolegijos gali būti pateikti ikiteisminio tyrimo įstaigai, prokurorui ar teismui dėl administracinių, civilinių, baudžiamųjų bylų kaip įrodymai arba kitais teisės aktų nustatytais atvejais. Kolegija gali pateikti asmens duomenis savo duomenų tvarkytojams, kurie	

teikia Kolegijai paslaugas ir tvarko asmens duomenis Kolegijos vardu. Duomenų tvarkytojai turi teisę tvarkyti asmens duomenis tik pagal Kolegijos nurodymus ir tik ta apimtimi, kiek tai yra būtina siekiant tinkamai vykdyti sutartyje nustatytus įsipareigojimus. Kolegija pasitelkia tik tuos duomenų tvarkytojus, kurie pakankamai užtikrina, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų BDAR reikalavimus ir būtų užtikrinta duomenų subjekto teisių apsauga.

V SKYRIUS
DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI

1. Teisės aktų nustatytais atvejais, Kolegija privalo sudaryti ir tvarkyti DTVĮ, kurie būtini tam, kad Kolegija turėtų nuolatinę ir aktualią informaciją apie savo vykdomos duomenų tvarkymo veiklos apimtis, joje dalyvaujančius asmenis, naudojamas tvarkymo priemones.
2. DTVĮ sudarymo formą ir formatą parengia Pareigūnas arba įgaliotas Kolegijos darbuotojas, atsižvelgdamas į Priežiūros institucijos rekomendacijas.
3. DTVĮ yra Kolegijos vidaus dokumentai, kuriuose gali būti konfidencialios informacijos. Todėl DTVĮ negali būti viešinami ir turi būti saugomi kaip ir kita Kolegijos konfidenciali informacija.
4. Siekiant užtikrinti Kolegijos atitikties BDAR įrodymus, už DTVĮ sudarymo, keitimo ir atnaujinimo organizavimą ir centralizuotą jų tvarkymą atsakingas Pareigūnas arba įgaliotas Kolegijos darbuotojas. Kolegijos vadovo įgaliotas darbuotojas yra tiesiogiai atsakingas už informacijos, reikalingos DTVĮ sudaryti, pakeisti ar atnaujinti, surinkimą, jų projektų paruošimą bei pateikimą Pareigūnui arba Kolegijos vadovo įgaliotam darbuotojai.
5. Kai Kolegijoje pradedamas ar keičiamas veiklos procesas ar funkcija susiję su duomenų tvarkymu, Kolegijos vadovas turi užtikrinti, kad apie tokį procesą ar jų pokyčius būtų surinkta visa informacija, reikalinga DTVĮ parengti ar pakeisti.
6. DTVĮ yra tvarkomi raštu. Rašytinei formai yra prilyginama ir elektroninė forma, saugoma kompiuteryje.
7. Tvarkant DTVĮ turi būti užtikrinamas jų pakeitimų atsekamumas, tam kad būtų galima nustatyti, kokie pakeitimai buvo daromi DTVĮ, kada jie buvo atlikti ir dėl kokių priežasčių.
8. DTVĮ yra tikrinami ir atnaujinami pagal poreikį, kad atitiktų realią asmens duomenų tvarkymo situaciją Kolegijoje.
9. DTVĮ turi būti pateikiami Priežiūros institucijai gavus jos prašymą. Už DTVĮ pateikimą atsakingas Pareigūnas arba Kolegijos vadovo įgaliotas darbuotojas.

VI SKYRIUS
VAIZDO DUOMENŲ TVARKYMAS

1. Kolegija, siekdama užtikrinti darbuotojų, studentų ir klientų saugumą, apsaugoti Kolegijos turtą nuo vagysčių ar sugadinimo, tvarko duomenų subjektų vaizdo duomenis darydama vaizdo įrašus.	
2. Vaizdo stebėjimas vykdomas adresu (-ais):	Marijampolės sav. Marijampolės m. P. Armino g. 92-4.
3. Duomenų subjektai apie vykdomą vaizdo stebėjimą informuojami informaciniais ženklais, įrengtais prieš duomenų subjektams patenkant į vaizdo stebėjimo lauką. Informaciniuose ženkluose pateikiama informacija apie tai, kad vykdomas vaizdo stebėjimas, nurodomas vaizdo stebėjimo tikslas, duomenų valdytojo pavadinimas, kontaktinė informacija (adresas, el. pašto adresas ir (arba) telefono ryšio numeris) ir nuoroda į interneto svetainę, kurioje galima rasti detalesnę informaciją apie asmens duomenų tvarkymą ir duomenų subjektų teisių įgyvendinimą.	
4. Vaizdo duomenys vaizdo duomenų įrašymo įrenginiuose saugomi 30 (trisdešimt) kalendorinių dienų, o nustačius pažeidimą – iki tyrimo pabaigos.	
5. Vaizdo duomenys fiksuojami šiomis vaizdo stebėjimo kameromis:	5.1. Kolegijos pastato lauko teritorijoje įrengtomis vaizdo stebėjimo kameromis – 5 vnt. (penki vienetai): 5.1.1. trys kameros, fiksuojančios automobilių stovėjimo aikštelės; 5.1.2. viena kamera, fiksuojanti pagrindinį įėjimą į bendrabutį; 5.1.3. viena kamera, fiksuojanti vaizdą bendrabučio viduje.
6. Duomenų subjektų interesai ir teisė į duomenų apsaugą ir privatumą nėra viršesni už Kolegijos interesus dėl šių priežasčių:	6.1. tvarkant asmens duomenis nėra tvarkoma informacija, susijusi su duomenų subjektų privačiu gyvenimu; 6.2. vaizdo stebėjimas Kolegijos patalpose vykdomas nedideliu mastu; 6.3. asmens duomenys nėra naudojami darbuotojų darbo kokybei vertinti; 6.4. nėra tvarkomi specialių kategorijų asmens duomenys.
7. Kolegijos vadovo įgaliotas tvarkyti vaizdo duomenis darbuotojas privalo:	7.1. užtikrinti, kad į stebimą erdvę nepatektų gyvenamosios patalpos, įėjimai į jas, joms priklausančios teritorijos, patalpos, kuriose asmenys pagrįstai tikisi absoliučios privatumo apsaugos ir kur toks stebėjimas žemintų žmogaus orumą; 7.2. užtikrinti, kad vaizdo stebėjimo sistema būtų techniškai tvarkinga, techniniai šios sistemos sutrikimai būtų šalinami operatyviai, panaudojant visus turimus techninius resursus; 7.3. užtikrinti kompiuterinės įrangos apsaugą nuo kenksmingos programinės įrangos; 7.4. imtis priemonių, kad būtų užkirstas kelias atsitiktiniam ar neteisėtam vaizdo duomenų sunaikinimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam tvarkymui; 7.5. saugoti vaizdo duomenų įrašymo įrenginiuose esančius duomenis; 7.6. užtikrinti, kad stebėjimo priemonių vaizdas nebūtų prieinamas pašaliniams asmenims; 7.7. neatskleisti, neperduoti ir nesudaryti sąlygų bet kokiomis priemonėmis susipažinti su vaizdo duomenimis tam teisės neturintiems asmenims; 7.8. nedelsdamas pranešti Kolegijos vadovui apie bet kokią įtartiną situaciją, kuri gali kelti grėsmę Kolegijos tvarkomų vaizdo duomenų saugumui; 7.9. laikytis kitų šiose Taisyklėse ir asmens duomenų apsaugą

	reglamentuojančiuose teisės aktuose nustatytų reikalavimų.
8. Kolegijos vadovo įgaliotas tvarkyti vaizdo duomenis darbuotojas turi teisę:	8.1. tiek stebėti tiesioginį kamerų vaizdą, tiek peržiūrėti įrašytus vaizdo įrašus, taip pat ištrinti, perkelti, nukopijuoti vaizdo įrašus, peržiūrėti darbuotojų judėjimo po Kolegijos teritoriją ir patalpas duomenis; 8.2. atlikti vaizdo stebėjimo sistemos priemonių techninę priežiūrą bei tikrinti įrašų kokybę. Šią teisę taip pat turi ir techninę priežiūrą atliekantys duomenų tvarkytojo darbuotojai; 8.3. kontroliuoti vaizdo stebėjimą, išskyrus atvejus, kai sistemoje yra techniniai gedimai arba atliekami profilaktiniai darbai.
9. Tiesioginį vaizdo įrašą gali stebėti:	9.1. Kolegijos bendrabučio administratorius; 9.2. Infrastruktūros ir paslaugų skyriaus vadovas.
10. Įgalioti asmenys ar kiti Kolegijos darbuotojai, pastebėję ar įtarę asmens duomenų saugumo pažeidimą, pastebėję, kad tvarkomi asmens duomenys tapo prieinami (kėsinamasi prie jų prieiti) asmenų, kurie neturi teisės tvarkyti tvarkomų asmens duomenų, turi nedelsiant imtis visų įmanomų priemonių neteisėtai prieigai prie tvarkomų asmens duomenų nutraukti ir nedelsiant informuoti savo tiesioginį vadovą arba ūkio skyriaus vedėją.	

VII SKYRIUS
REIKALAVIMAI DARBUOTOJAMS, TVARKANTIEMS ASMENS DUOMENIS IR JŲ ATSAKOMYBĖ

1. Darbuotojas, tvarkantis duomenų subjektų asmens duomenis, privalo:	1.1. laikytis su asmens duomenų tvarkymu susijusių principų ir saugumo reikalavimų, įtvirtintų BDAR, ADTAĮ, šiose Taisyklėse ir kituose teisės aktuose, reglamentuojančiuose asmens duomenų tvarkymą ir privatumo apsaugą; 1.2. laikytis konfidencialumo principo ir laikyti paslaptyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jis susipažino vykdydamas savo funkcijas, nebent tokia informacija būtų vieša pagal galiojančių įstatymų ar kitų teisės aktų nuostatas. Kolegijos darbuotojai, kurie tvarko asmens duomenis arba kuriems Kolegijos vadovo įsakymo pagrindu suteikti įgaliojimai ir / arba prieiga prie asmens duomenų, privalo pasirašyti Darbuotojo įsipareigojimą saugoti asmens duomenis ir duomenis tvarkyti tik tokia apimtimi, kiek tai susiję su jų darbo funkcijomis. Pareiga saugoti asmens duomenų paslaptį galioja ir perėjus dirbti į kitas pareigas ar pasibaigus darbo santykiams; Konfidencialumo taisyklė taikoma tiek tais atvejais, kuomet darbuotojui prieigą prie asmens duomenų suteikė Kolegija, tiek tais atvejais, kuomet darbuotojas pats sužinojo asmens duomenis. 1.3. laikytis Taisyklėse nustatytų techninių ir organizacinių asmens duomenų saugumo priemonių, kad būtų užkirstas kelias atsitiktiniam ar neteisėtam asmens duomenų sunaikinimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam tvarkymui, saugoti dokumentus, duomenų rinkmenas bei duomenų bazėse saugomus duomenis ir vengti nereikalingų kopijų darymo; Dokumentų kopijos, kuriose nurodomi duomenų subjekto duomenys, turi būti sunaikinamos tokiu būdu, kad šių dokumentų nebūtų galima atkurti ir atpažinti jų turinio; 1.4. neatskleisti, neperduoti ir nesudaryti sąlygų bet kokiomis priemonėmis susipažinti su asmens duomenimis nė vienam asmeniui, kuris nėra įgaliotas tvarkyti asmens duomenis (švaraus stalo politika); Jeigu darbuotojui kyla abejonių, ar konkretus duomenų subjektas turi teisę gauti asmens duomenis, jis privalo konsultuotis su Pareigūnu arba Kolegijos vadovo įgaliotu darbuotoju ir tik gavęs teigiamą atsakymą turi teisę pateikti asmens duomenis; 1.5. darbuotojai turi teisę ir pareigą nedelsiant pranešti tiesioginiam vadovui, Pareigūnui arba Kolegijos vadovo įgaliotam darbuotojui, apie bet kokią įtartiną situaciją, pastebėtus neteisėto asmens duomenų tvarkymo atvejus (įskaitant šių Taisyklių pažeidimus) kurie gali kelti grėsmę Kolegijos tvarkomų asmens duomenų saugumui; 1.6. laikytis kitų Taisyklėse ir asmens duomenų apsaugą reglamentuojančiuose teisės aktuose nustatytų reikalavimų.
2. Darbuotojas netenka teisės tvarkyti asmens duomenis, kai pasibaigia jo darbo santykiai su Kolegija arba kai jam pavedama vykdyti su duomenų tvarkymu nesusijusias funkcijas.	

VIII SKYRIUS
TECHNINĖS IR ORGANIZACINĖS DUOMENŲ SAUGUMO PRIEMONĖS

<table>
<tr><td colspan="2">1. Kolegija, saugodama asmens duomenis, įgyvendina ir užtikrina tinkamas organizacines ir technines priemones, skirtas apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo. Nustačius asmens duomenų saugumo pažeidimus, Kolegija imasi neatidėliotinų priemonių užkirsti kelią neteisėtam asmens duomenų tvarkymui.</td></tr>
<tr><td colspan="2">2. Kolegija, atsižvelgiant į darbuotojo einamas pareigas, savo nuožiūra darbuotojams suteikia darbo priemones. Kolegijai priklausančios Informacinės ir komunikacinės technologijos, t. y. kompiuteriai, mobilieji telefonai, prieiga prie interneto, elektroninis paštas, spausdintuvai, duomenų laikmenos ir kiti prietaisai, yra skirtos išimtinai darbuotojų darbo funkcijoms vykdyti, jeigu Kolegija su darbuotoju nesusitaria kitaip.</td></tr>
<tr><td>3. Siekiant apsaugoti duomenų subjekto duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, nuo bet kokio kito neteisėto tvarkymo turi būti taikomos tokios organizacinės ir techninės priemonės:</td><td>3.1. Infrastruktūrinės priemonės: tinkamas techninės įrangos išdėstymas ir priežiūra, informacinių duomenų saugojimo priemonių fizinių ir programinių saugumo priemonių įgyvendinimas, griežtas priešgaisrinės apsaugos tarnybų nustatytų normų laikymasis ir kt.;
3.2. Administracinės priemonės: tinkamas darbo organizavimas, informacinių sistemų priežiūra;
3.3. Telekomunikacinės priemonės: tinklo valdymas, naudojimosi internetu saugumo užtikrinimas ir kt.</td></tr>
<tr><td>4. Darbuotojai privalo taip organizuoti savo darbą, kad kiek įmanoma apribotų galimybę kitiems asmenims (kitiems Kolegijos darbuotojams, praktikantams, savanorišką praktiką atliekantiems ar kitiems tretiesiems asmenims) sužinoti tvarkomus asmens duomenis. Ši nuostata įgyvendinama:</td><td>4.1. nepaliekant dokumentų, su tvarkomais asmens duomenimis ar kompiuterio, kuriuo naudojantis galima atidaryti rinkmenas su asmens duomenimis, be priežiūros taip, kad juose esančią informaciją galėtų perskaityti darbuotojai, neturintys teisės dirbti su konkrečiais asmens duomenimis ar kiti asmenys;
4.2. dokumentus laikant taip, kad jų (ar jų fragmentų) negalėtų perskaityti atsitiktiniai asmenys;
4.3. jei dokumentai, kuriose yra asmens duomenų, kitiems darbuotojams, įstaigoms perduodami per asmenis, kurie neturi teisės tvarkyti asmens duomenis, arba per paštą ar kurjerį, jie privalo būti perduodami užklijuotame nepermatomame voke. Šis punktas netaikomas, jeigu minėti pranešimai įteikiami klientams, kitiems interesantams asmeniškai ir konfidencialiai.</td></tr>
<tr><td>5. Darbuotojams, naudojantiems elektroninį paštą, interneto prieigą ir kitą informacinių technologijų ir telekomunikacijų įrangą, draudžiama:</td><td>5.1. siųsti elektroninio pašto žinutes, naudojantis kito asmens arba neegzistuojančiu elektroninio pašto adresu;
5.2. siųsti elektroninio pašto žinutes, nuslepiant savo tapatybę;
5.3. negavus Kolegijos vadovo sutikimo, siųsti elektroninius laiškus, kuriuose yra informacija pripažįstama konfidencialia informacija ar Kolegijos komercine paslaptimi, išskyrus, jei informacija siunčiama asmeniui, kuris turi teisę gauti šią informaciją;
5.4. negavus Kolegijos vadovo sutikimo perduoti, platinti, atskleisti tretiesiems asmenims darbui su technine ir programine įranga jiems suteiktus prieigos vardus, slaptažodžius ar kitus duomenis;
5.5. kurti ar platinti laiškus, skatinančius gavėją siųsti laiškus kitiems. Laiškai su perspėjimais dėl kompiuterinių virusų, telefonų pasiklausymų ar kitų tariamų reiškinių, kuriuose prašoma nusiųsti gautą laišką visiems savo kolegoms, draugams ar pažįstamiems, turi</td></tr>
</table>

	būti nedelsiant ištrinami. Jei pranešimas sukelia įtarimų, prieš jį pašalinant, pranešti tiesioginiam vadovui; 5.6. naudoti interneto prieigą ir elektroninį paštą asmeniniams tikslams, Lietuvos Respublikos įstatymais draudžiamai veiklai, šmeižiančio, įžeidžiančio, grasinančiojo pobūdžio ar visuomenės dorovės ir moralės principams prieštaraujančiai informacijai, kompiuterių virusams, masinei nepageidaujamai informacijai „spam“ siųsti ar kitiems tikslams, galintiems pažeisti Kolegijos ar kitų asmenų teisėtus interesus; 5.7. atlikti veiksmus, pažeidžiančius fizinio ar juridinio asmens teises, kurias saugo autorių, gretutinių ir intelektinės nuosavybės teisių apsaugos įstatymai. Tarp tokių veiksmų yra programinės įrangos diegimas, naudojimas, saugojimas arba platinimas neturint licencijos, neleistinas autorių teisėmis apsaugotų kūrinių kopijavimas; 5.8. parsisiųsti arba platinti tiesiogiai su darbu nesusijusią grafinę, garso ir vaizdo medžiagą, žaidimus ir programinę įrangą, siųsti duomenis, kurie užkrėsti virusais, turi įvairius kitus programinius kodus, bylas, galinčias sutrikdyti kompiuterinių ar telekomunikacinių įrenginių bei programinės įrangos funkcionavimą ir saugumą; 5.9. atskleisti prisijungimo prie Kolegijos sistemų informaciją (prisijungimo vardą, slaptažodį) arba leisti naudotis savo prisijungimo vardu kitiems asmenims; **Dirbant su slaptažodžiais reikia laikytis taisyklių:** 5.9.1. saugoti slaptažodį. Neužrašinėti jo ant popieriaus skiaučių, kalendorių ir pan. Nepalikti lapelio su slaptažodžiu priklijuoto prie vaizduoklio arba prie apatinės darbo stalo pusės; 5.9.2. nenaudoti trumpų ir elementarių slaptažodžių sudarytų iš reikšminių žodžių; 5.10. apeiti ar kitaip pažeisti bet kurio kompiuterio, tinklo ar paskyros autentifikacijos arba saugumo sistemas; 5.11. ardyti ar išmontuoti ar kitaip keisti kompiuterinę įrangą; 5.12. perkopijuoti programinę įrangą; 5.13. savarankiškai šalinti kompiuterinės įrangos gedimus; 5.14. parsisiųsti ar žaisti internetinius ar kitus kompiuterinius žaidimus; 5.15. savavališkai blokuoti antivirusines programas ar kitas programas; 5.16. sutrikdyti kompiuterinės sistemos darbą arba panaikinti galimybę naudotis teikiama paslauga ar informacija; 5.17. dalyvauti interneto lažybose ir azartiniuose lošimuose; 5.18. naudoti Kolegijos išteklius komercinei veiklai vystyti ar naudai gauti; 5.19. savavališkai keisti kompiuterių ar kitų prietaisų tinklo parametrus (IP adresą ir pan.), savarankiškai keisti, taisyti informacinių technologijų ir telekomunikacijų techninę ir programinę įrangą; 5.20. pažeisti kitų tinklų, kurių paslaugomis naudojamasi, naudojimo arba ekvivalentiškas taisykles; 5.21. savavališkai keisti interneto naršyklės ir elektroninio pašto programinės įrangos parametrus, susijusius su apsauga arba

	prisijungimo būdu, nepaisyti bet kurio iš įdiegtų saugumo mechanizmų; 5.22. atlikti bet kokius kitus su darbo funkcijų vykdymu nesusijusius ir teisės aktams prieštaraujančius veiksmus; 5.23. neįgaliotiems asmenimis Kolegijoje ar už Kolegijos ribų naudoti ir perduoti slaptažodžius ir kitus duomenis, kuriais pasinaudojus programinėmis ir techninėmis priemonėmis galima sužinoti Kolegijos duomenis ar kitaip sudaryti sąlygas susipažinti su Kolegijos duomenimis.
6. Keitimosi informacija politika	6.1. Perduodant informaciją elektroniniu paštu, būtina: 6.1.1. atidžiai užrašyti adresato elektroninio pašto adresą, kad informacija nebūtų perduota kitam asmeniui; 6.1.2. už organizacijos ribų siunčiamiems laiškams naudoti el. pašto programoje numatytą el. laiško parašą (angl. „signature“) ir jo nekeisti; 6.1.3. priimant sprendimus pagal elektroniniu paštu gautą informaciją, būtina įsitikinti šios informacijos tikrumu (kitas asmuo gali apsimesti tikruoju siuntėju). Kilus įtarimui bei svarbiais atvejais rekomenduojama susisiekti su siuntėju ir įsitikinti ar gautas laiškas buvo jo išsiųstas; 6.2. neatverti pridėtų (angl. „attached“) failų, kurie yra gauti iš nepažįstamų asmenų, arba nėra galimybės įsitikinti šių failų turiniu; 6.3. už pašalinių asmenų naudojimąsi internetu kompiuteryje ir informacijos perdavimą elektroniniu paštu yra atsakingas kompiuterio naudotojas.
7. Bendros apsaugos nuo virusų taisyklės:	7.1. prieš naudojant nežinomas išorines duomenų laikmenas arba kurios buvo naudojamos kitame kompiuteryje, būtina atlikti jų antivirusinę profilaktiką; 7.2. kilus įtarimui patikrinti kompiuterį nuo virusų; 7.3. siekiant išvengti kompiuterinių virusų, nepaleisti nežinomų programų. Gavus nežinomų siuntėjų atsiųstų elektroninių laiškų priedus, kuriuose gali būti kompiuterinių virusų, darbuotojas privalo neatidaryti gautų elektroninių laiškų priedų ir informuoti tiesioginį arba Kolegijos vadovą; 7.4. darbuotojas, pastebėjęs virusų atakos požymius, privalo išjungti kompiuterį ir kreiptis į tiesioginį arba Kolegijos vadovą.
8. Kolegija pasilieka teisę be atskiro darbuotojo įspėjimo riboti prieigą prie atskirų interneto svetainių ar programinės įrangos. Nepakankant minėtų priemonių, Kolegija gali tikrinti, kaip darbuotojas laikosi elektroninio pašto ir interneto resursų naudojimo reikalavimų nurodytais tikslais, tiriant incidentus, atiduoti darbuotojų naudojamą įrangą tirti tretiesiems asmenims, kurie teisės aktų nustatyta tvarka turi teisę tokius duomenis gauti.	
9. Kolegija neužtikrina darbuotojų asmeninės informacijos konfidencialumo darbuotojams, naudojantiems elektroninį paštą ir interneto resursus asmeniniais tikslais. Kolegija turi teisę neįspėjus darbuotojo atidaryti šiam priskirtą darbinę elektroninio pašto dėžutę ir skaityti elektroninius laiškus tada, jei yra pagrindo manyti, kad darbuotojo elektroninio pašto dėžutėje yra netinkamo, įstatymus ar Kolegijos teisės interesus pažeidžiančio turinio informacija arba egzistuoja teisėta su darbo santykiais susijusi priežastis atlikti šiuos veiksmus.	
10. Kolegijos vadovas neužtikrina, kad bus išsaugotas privatumas to, ką Kolegijos darbuotojai sukuria, siunčia ar gauna Kolegijos informacinėje sistemoje.	
11. Jeigu Kolegijos darbuotojas abejoja įdiegtų saugumo priemonių patikimumu, jis turi kreiptis į tiesioginį arba Kolegijos vadovą, kad būtų įvertintos turimos saugumo priemonės ir, jei reikia, inicijuotas papildomų priemonių įsigijimas ir įdiegimas.	

IX SKYRIUS
ASMENS DUOMENŲ TVARKYMUI TAIKOMŲ SAUGUMO PRIEMONIŲ SĄRAŠAS

Nr.	Priemonės
1.	nedarbo metu Kolegijos patalpos rakinamos
2.	Kolegijos patalpose esantys kabinetai rakinami, raktus turi tik tame kabinete dirbantys darbuotojai, apsauga ir Kolegijos administracija
3.	įrengta patalpų signalizacijos sistema
4.	patekimas prie serverių įrangos, kuriose saugomi duomenys, yra apribotas fizinėmis priemonėmis (rakinama atskira patalpa), į kurią gali patekti tik įgalioti asmenys
5.	prieiga prie duomenų suteikiama tik tam asmeniui, kuriam duomenys yra reikalingi jo funkcijoms vykdyti (būtinumo žinoti principas)
6.	vidinis tinklas apsaugotas ugnies sienomis
7.	kontroliuojamas darbuotojų prisijungimas prie vidinio tinklo
8.	kontroliuojamas trečiųjų šalių vartotojų prisijungimas
9.	apribota programinė prieiga prie duomenų
10.	darbuotojų kompiuteriuose naudojami slaptažodžiai. Darbuotojas, dirbantis konkrečiu kompiuteriu, gali žinoti tik savo slaptažodį, privalo saugoti suteiktą slaptažodį ir neatskleisti jo tretiesiems asmenims. Slaptažodžiai esant būtinybei (pasikeitus darbuotojui, iškilus įsilaužimo grėsmei ir pan.) turi būti keičiami periodiškai, **ne rečiau kaip kartą per tris mėnesius**, o taip pat susidarius tam tikroms aplinkybėms (pvz.: pasikeitus darbuotojui, iškilus įsilaužimo grėsmei, kilus įtarimui, kad slaptažodis tapo žinomas tretiesiems asmenims, ir pan.). Slaptažodžiai neturi sutapti su darbuotojo ar su jo šeimos narių asmeniniais duomenimis
11.	užtikrinamas saugių protokolų (pvz., SSL, SDB) ir (arba) slaptažodžių naudojimas, kai asmens duomenys perduodami išoriniais duomenų perdavimo tinklais
12.	naudojama sertifikuota programinė įranga
13.	programinė įranga atnaujinama, laikantis nustatytos tvarkos
14.	kompiuteriuose įdiegtos antivirusinės programos, kurios nuolat atnaujinamos
15.	IT sistemos turi nustatytą sesijos laiką, t. y. naudotojui esant neaktyviam, neveiksniam sistemoje nustatytą laiką, jo sesija yra nutraukiama ne vėliau kaip po 15 minučių neaktyvios sesijos
16.	darbuotojams nesuteiktos teisės savavališkai keisti jam priskirtos kompiuterinės įrangos (monitoriai, skeneriai, spausdintuvai bei kopijavimo aparatų spausdinimo valdikliai, klaviatūros, pelės, kolonėlės, ausinės, vaizdo kameros bei fotokameros, multimedijos projektoriai ir pan.) ir įdiegtos programinės įrangos
17.	nesant būtinybės, rinkmenos su fizinių asmenų duomenimis neturi būti dauginamos skaitmeniniu būdu, t. y. kuriamos rinkmenų kopijos vietiniuose kompiuterių diskuose, nešiojamose laikmenose, nuotolinėse rinkmenų talpyklose ir kt.
18.	už Kolegijos duomenų bazėse ir IT sistemose esančių duomenų sunaikinimą atsakingi šias sistemas administruojantys darbuotojai
19.	darbuotojai mokomi dirbti su programine įranga
20.	ne rečiau kaip 1 (vieną) kartą per kalendorinius metus numatytas darbuotojų mokymas duomenų saugos klausimais
21.	daromos atsarginės duomenų kopijos

22.	įranga prižiūrima pagal gamintojo rekomendacijas
23.	priežiūrą ir gedimų šalinimą atlieka kvalifikuoti specialistai
24.	stebima duomenų perdavimo tinklo būklė
25.	svarbiausios kompiuterinės įrangos techninė būklė nuolat stebima
26.	tinkamai suplanuotos ir įrengtos svarbiausios kompiuterinės įrangos laikymo patalpos
27.	įrengta vandens nutekėjimo sistema
28.	patalpose yra ugnies gesintuvų
29.	pastato patalpose įrengti dūmų ir temperatūros jutikliai
30.	svarbiausiai kompiuterinei įrangai skirti nenutrūkstamo maitinimo šaltiniai
31.	elektros ir duomenų kabeliai saugiai atskirti

X SKYRIUS
ASMENS DUOMENŲ TVARKYTOJAI IR GAVĖJAI

1. Tais atvejais, kai Kolegija įgalioja duomenų tvarkytoją atlikti asmens duomenų tvarkymo veiksmus, tarp Kolegijos ir duomenų tvarkytojo turi būti sudaroma duomenų tvarkymo sutartis.
2. Sprendimą perduoti duomenų subjekto duomenų tvarkymą asmens duomenų tvarkytojui priima Kolegijos vadovas.
3. Kolegija parenka duomenų tvarkytoją, kuris užtikrina, kad būtų įgyvendintos techninės ir organizacinės duomenų apsaugos priemonės, skirtos apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo, įgyvendinant ir užtikrinant tokių priemonių laikymąsi.
4. Kolegija, sutartimi įgaliodama duomenų tvarkytoją tvarkyti asmens duomenis, nurodo, kad asmens duomenys būtų tvarkomi atsižvelgiant į asmens duomenų tvarkymą reglamentuojančius teisės aktus, Kolegijos nurodymus, taip pat nurodant, kokius asmens duomenų tvarkymo veiksmus privalo atlikti duomenų tvarkytojas Kolegijos vardu, duomenų tvarkytojo įsipareigojimai Kolegijai, įskaitant įsipareigojimą laikytis ADTAĮ įtvirtintų reikalavimų, duomenų tvarkymo trukmė, pobūdis, asmens duomenų rūšis, duomenų subjektų kategorijos, duomenų tvarkytojo pareiga ištrinti arba grąžinti Kolegijai asmens duomenis, jų kopijas, pabaigus Kolegijai teikti paslaugas.
5. Kolegija, sudarydama sutartį su duomenų tvarkytoju, be kita ko, nurodo, kad duomenų tvarkytojas privalo užtikrinti Kolegijos perduodamų tvarkyti duomenų konfidencialumą, o ketindamas tvarkymui pasitelkti trečiuosius asmenis (kitus duomenų tvarkytojus), duomenų tvarkytojas privalo gauti išankstinį rašytinį Kolegijos pritarimą.
6. Duomenų valdytojo tvarkomi duomenys duomenų gavėjams, kurie po duomenų perdavimo asmens duomenis tvarko savarankiškais tikslais, o ne pagal duomenų valdytojo nurodymus, teikiami tokią pareigą teikti duomenis numatant teisės aktui, esant duomenų subjekto sutikimui arba kitam teisėto duomenų teikimo (tvarkymo) pagrindui.
7. Duomenų teikimas duomenų gavėjui turi būti būtinas pasiekti duomenų tvarkymo tikslui, nustatytam prieš renkant duomenis, arba turi egzistuoti tinkamas teisinis pagrindas duomenis tvarkyti ir teikti nauju tikslu.
8. Duomenų valdytojo įgaliotų duomenų tvarkytojų ir jų atliekamų funkcijų, taip pat duomenų gavėjų sąrašas pateikiamas Tvarkymo veiklos įrašuose. Pasitelkus naują duomenų tvarkytoją ar pradėjus teikti duomenis naujam duomenų gavėjui, Tvarkymo veiklos įrašas papildomas nauja informacija. Atitinkamai, atsisakius duomenų tvarkytojo paslaugų ar pasikeitus duomenų gavėjui, taip pat padaromi atitinkami pokyčiai Tvarkymo veiklos įrašuose.

XI SKYRIUS
DUOMENŲ SUBJEKTŲ TEISĖS IR JŲ ĮGYVENDINIMO TVARKA

1. Duomenų subjektai turi šias teises:	**1.1. gauti informaciją apie asmens duomenų tvarkymą:** 1.1.1. informacija apie Kolegijoje atliekamą duomenų subjektų asmens duomenų tvarkymą, nurodyta BDAR 13 ir 14 str., duomenų subjektui pateikiama žodžiu, raštu arba elektroninių ryšių priemonėmis (duomenų subjekto kreipimosi į Kolegiją būdu), taip pat skelbiama Kolegijos interneto svetainės Privatumo politikoje ir skiltyje „Asmens duomenų apsauga“. 1.1.2. informacija apie duomenų subjektų asmens duomenų tvarkymą pateikiama asmens duomenų gavimo metu. 1.1.3. kai duomenų subjekto asmens duomenys renkami ne tiesiogiai iš duomenų subjekto, apie šio duomenų subjekto asmens duomenų tvarkymą informuojama: 1.1.3.1. per pagrįstą laikotarpį nuo asmens duomenų gavimo, bet ne vėliau kaip per vieną mėnesį, atsižvelgiant į konkrečias asmens duomenų tvarkymo aplinkybes; 1.1.3.2. jeigu asmens duomenys bus naudojami ryšiams su duomenų subjektu palaikyti – ne vėliau kaip pirmą kartą susisiekiant su tuo duomenų subjektu; arba 1.1.3.3. jeigu numatoma asmens duomenis atskleisti kitam duomenų gavėjui – ne vėliau kaip atskleidžiant duomenis pirmą kartą. **1.2. susipažinti su savo asmens duomenimis:** 1.2.1. Kolegija, esant duomenų subjekto prašymui įgyvendinti teisę susipažinti su savo asmens duomenimis, turi pateikti: 1.2.1.1. informaciją, ar duomenų subjekto asmens duomenys tvarkomi; 1.2.1.2. su asmens duomenų tvarkymu susijusią informaciją, numatytą BDAR 15 str. 1 ir 2 d., jeigu duomenų subjekto asmens duomenys tvarkomi; 1.2.1.3. tvarkomų asmens duomenų kopiją. 1.2.2. tvarkomus duomenis duomenų subjektui teikti raštu ir neatlygintinai. Tam tikrais atvejais (kai duomenų subjektas akivaizdžiai piktnaudžiauja savo teisėmis, nepagrįstai arba neproporcingai, pakartotinai teikia prašymus dėl jų pasikartojančio turinio pateikti informaciją, išrašus, dokumentus), toks informacijos ir duomenų teikimas duomenų subjektui gali būti apmokestintas, t. y. duomenų valdytojas gali imti pagrįstą mokestį, atsižvelgdamas į informacijos teikimo arba pranešimų ar veiksmų, kurių prašoma, administracines išlaidas; arba gali atsisakyti imtis veiksmų pagal prašymą. Duomenų valdytojui tenka pareiga įrodyti, kad prašymas yra akivaizdžiai nepagrįstas arba neproporcingas; 1.2.3. informaciją pateikti įprastai naudojama elektronine forma, nebent prašoma informaciją pateikti kitaip. **1.3. reikalauti ištaisyti netikslius duomenis ar papildyti neišsamius duomenis:** 1.3.1. duomenų subjektas, vadovaudamasis BDAR 16 str., turi teisę reikalauti, kad duomenų valdytojas nepagrįstai nedelsdamas ištaisytų netikslius su juo susijusius asmens duomenis. Atsižvelgiant į tikslus, kuriais duomenys buvo tvarkomi, duomenų subjektas turi teisę reikalauti, kad būtų papildyti neišsamūs asmens duomenys pateikdamas papildomą prašymą;

	1.3.2. siekdama įsitikinti, kad tvarkomi duomenų subjekto asmens duomenys yra tikslūs ar išsamūs, Kolegija gali duomenų subjekto paprašyti pateikti tai patvirtinančius įrodymus. 1.3.3. kiekvienam duomenų gavėjui, kuriam buvo atskleisti asmens duomenys, duomenų valdytojas praneša apie bet kokį asmens duomenų ištaisymą, ištrynimą arba tvarkymo apribojimą, nebent to padaryti nebūtų įmanoma arba tai pareikalautų neproporcingų pastangų. Duomenų subjektui paprašius, duomenų valdytojas informuoja duomenų subjektą apie tuos duomenų gavėjus. **1.4. nesutikti, kad būtų tvarkomi jo asmens duomenys:** 1.4.1. duomenų subjektas, vadovaudamasis BDAR 21 str., turi teisę dėl su jo konkrečiu atveju susijusių priežasčių bet kuriuo metu nesutikti, kad Kolegija tvarkytų jo asmens duomenis, išskyrus šiuos atvejus: 1.4.1.1. tvarkyti asmens duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas; 1.4.1.2. tvarkyti duomenis būtina siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų, išskyrus atvejus, kai tokie duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą, yra už juos viršesni, ypač kai duomenų subjektas yra vaikas. 1.4.2. Duomenų subjektui išreiškus nesutikimą dėl asmens duomenų tvarkymo, toks tvarkymas atliekamas tik tuo atveju, jeigu motyvuotai nusprendžiama, kad priežastys, dėl kurių tvarkomi asmens duomenys, yra viršesnės už duomenų subjekto interesus, teises ir laisves, arba jeigu asmens duomenys yra reikalingi pareikšti, vykdyti ar apginti teisinius reikalavimus. **1.5. reikalauti ištrinti duomenis („Teisė būti pamirštam“):** 1.5.1. Duomenų subjekto teisė ištrinti jo asmens duomenis („teisė būti pamirštam“) įgyvendinama BDAR 17 str. numatytais atvejais. 1.5.2. Duomenų subjekto teisė reikalauti ištrinti asmens duomenis gali būti neįgyvendinta BDAR 17 str. 3 d. numatytais atvejais. 1.5.3. Jeigu duomenų subjekto asmens duomenys (ištrinti pagal duomenų subjekto prašymą) buvo perduoti duomenų gavėjams, Kolegija šiuos duomenų gavėjus apie tai informuoja, nebent tai būtų neįmanoma ar tam prireiktų neproporcingų pastangų. Duomenų subjektas turi teisę prašyti, kad jam būtų pateikta informacija apie tokius duomenų gavėjus. **1.6. į duomenų perkeliamumą:** 1.6.1. Kolegija įgyvendina duomenų subjekto teisę į duomenų perkeliamumą BDAR 20 str. numatytomis sąlygomis. 1.6.2. Duomenų subjektas teisės į duomenų perkeliamumą neturi tų asmens duomenų atžvilgiu, kurie tvarkomi neautomatiniu būdu susistemintose rinkmenose, pavyzdžiui, popierinėse bylose. 1.6.3. Duomenų subjektas, kreipdamasis dėl teisės į duomenų perkeliamumą, turi nurodyti, ar pageidauja, kad jo asmens duomenys būtų persiųsti jam ar kitam duomenų valdytojui. 1.6.4. Pagal duomenų subjekto prašymą perkelti jo asmens duomenys nėra automatiškai ištrinami. Jeigu duomenų subjektas to pageidauja, turi kreiptis į duomenų valdytoją dėl teisės reikalauti ištrinti duomenis („teisės būti pamirštam“) įgyvendinimo.

	1.7. apriboti asmens duomenų tvarkymą: 1.7.1. BDAR 18 str. 1 d. numatytais atvejais Kolegija privalo įgyvendinti duomenų subjekto teisę apriboti jo asmens duomenų tvarkymą. 1.7.2. Asmens duomenys, kurių tvarkymas apribotas, yra saugomi, o prieš tokio apribojimo panaikinimą duomenų subjektas raštu, žodžiu arba elektroninių ryšių priemonėmis yra informuojamas. 1.7.3. Jeigu duomenų subjekto asmens duomenys (kurių tvarkymas apribotas pagal duomenų subjekto prašymą) buvo perduoti duomenų gavėjams, Kolegija šiuos duomenų gavėjus apie tai informuoja, nebent tai būtų neįmanoma ar tam prireiktų pareikalautų neproporcingų pastangų. Duomenų subjektas turi teisę prašyti, kad jam būtų pateikta informacija apie tokius duomenų gavėjus. 1.8. Reikalauti, kad nebūtų taikomas tik automatizuotu asmens duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas: 1.8.1. Duomenų subjektas turi teisę reikalauti, kad jo atžvilgiu nebūtų taikomas tik automatizuotu duomenų tvarkymu grindžiamas sprendimas ir toks sprendimas būtų peržiūrėtas, vadovaujantis BDAR 22 str. 1.8.2. Duomenų subjektui kreipusis dėl automatizuotu asmens duomenų tvarkymu grindžiamo sprendimo peržiūros, duomenų valdytojas turi atlikti išsamų visų svarbių duomenų, įskaitant ir duomenų subjekto pateiktos informacijos, vertinimą.
2. Kolegija imasi tinkamų priemonių, jog informacija susijusi su duomenų tvarkymu, duomenų subjektui būtų pateikta glausta, skaidria, suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba.	
3. Duomenų subjektas dėl jo teisių įgyvendinimo privalo pateikti Kolegijai rašytinį prašymą, kuris turi būti:	3.1. įskaitomas, duomenų subjekto pasirašytas, naudojant laisvą prašymo formą ir formatą arba naudojant rekomenduojamą Kolegijos parengtą kreipimosi formą (Taisyklių priedas Nr. 2); 3.2. prašyme turi būti nurodyta: duomenų subjekto vardas, pavardė, kiti požymiai, leidžiantys identifikuoti asmenį, kontaktiniai duomenys ir informacija apie tai, kokią iš aukščiau nurodytų teisių ir kokios apimties duomenų subjektas pageidauja įgyvendinti, bei informacija, kokiu būdu pageidaujama gauti atsakymą.
4. Prašymą galima pateikti:	4.1. asmeniškai; 4.2. paštu ar per pasiuntinį; 4.3. per atstovą; 4.4. elektroninių ryšių priemonėmis.
5. Kolegija, duomenų subjekto prašymo, kuris pateiktas nesilaikant šiose Taisyklėse nustatytų reikalavimų, nenagrinėja.	
6. Pateikdamas prašymą, duomenų subjektas privalo patvirtinti savo tapatybę:	6.1. kai prašymas teikiamas tiesiogiai atvykus į Kolegiją – pateikti galiojantį asmens tapatybę patvirtinantį dokumentą; 6.2. kai prašymas siunčiamas paštu ar per pasiuntinį – pridėti notaro ar kita Lietuvos Respublikos teisės aktų nustatyta tvarka patvirtintą prašymą teikiančio asmens tapatybę patvirtinančio dokumento kopiją; 6.3. kai prašymas teikiamas per atstovą – pateikti Lietuvos Respublikos teisės aktų nustatyta tvarka atstovavimą patvirtinantį dokumentą ar įstatymų nustatyta tvarka patvirtintą atstovavimo dokumento kopiją; 6.4. kai prašymas teikiamas elektroninių ryšių priemonėmis – pasirašyti kvalifikuotu elektroniniu parašu.
7. Jei įmanoma, duomenų subjekto prašymu, informacija gali būti suteikta žodžiu, jeigu duomenų	

<table>
<tr><td colspan="2">subjekto tapatybe galima įsitikinti patikrinus duomenų subjekto nurodytą ir Kolegijos turimą informaciją (pavyzdžiui: vardas, pavardė, telefono numeris, lojalumo kortelės numeris gali būti pasakomi duomenų subjektui, jeigu duomenų subjektas prašo šią informaciją suteikti žodžiu, kreipdamasis į Kolegiją, ir jeigu yra techninė galimybė šią informaciją surinkti).</td></tr>
<tr><td colspan="2">8. Visi prašymai, kuriuos Kolegija bet kokiomis ryšio priemonėmis gauna dėl duomenų subjektų teisių įgyvendinimo turi būti perduoti ar persiųsti Pareigūnui. Visi Kolegijos darbuotojai, kurie prižiūri įeinančią komunikaciją, privalo užtikrinti, kad gauti duomenų subjektų prašymai būtų atpažinti ir perduoti Pareigūnui ir Kolegijos vadovo įgaliotam darbuotojui nedelsiant, ne vėliau kaip per 1 (vieną) darbo dieną</td></tr>
<tr><td>9. Duomenų subjektų teisių įgyvendinimo tvarka:</td><td>9.1. Duomenų valdytojas privalo suteikti duomenų subjektui informaciją:
9.1.1. per pagrįstą laikotarpį nuo asmens duomenų gavimo, bet ne vėliau kaip per vieną mėnesį nuo duomenų subjekto prašymo gavimo dienos, atsižvelgiant į konkrečias asmens duomenų tvarkymo aplinkybes;
9.1.2. jeigu asmens duomenys bus naudojami ryšiams su duomenų subjektu palaikyti – ne vėliau kaip pirmą kartą susisiekiant su tuo duomenų subjektu;
9.1.3. jeigu numatoma asmens duomenis atskleisti kitam duomenų gavėjui – ne vėliau kaip atskleidžiant duomenis pirmą kartą.
9.2. Duomenų valdytojas nepagrįstai nedelsdamas, tačiau bet kuriuo atveju ne vėliau kaip per vieną mėnesį nuo prašymo gavimo, pateikia duomenų subjektui informaciją (atsakymą) apie veiksmus, kurių imtasi gavus prašymą. Šis laikotarpis prireikus gali būti pratęstas dar dviem mėnesiams, atsižvelgiant į prašymų sudėtingumą ir skaičių. Duomenų valdytojas per vieną mėnesį nuo prašymo gavimo informuoja duomenų subjektą apie tokį pratęsimą, kartu pateikdamas vėlavimo priežastis. Kai duomenų subjektas prašymą pateikia elektroninės formos priemonėmis, informacija jam taip pat pateikiama, jei įmanoma, elektroninėmis priemonėmis, išskyrus atvejus, kai duomenų subjektas paprašo ją pateikti kitaip.
9.3. Jei duomenų valdytojas nesiima veiksmų pagal duomenų subjekto prašymą, duomenų valdytojas nedelsdamas, tačiau ne vėliau kaip per vieną mėnesį nuo prašymo gavimo, informuoja duomenų subjektą apie neveikimo priežastis ir apie galimybę pateikti skundą Priežiūros institucijai bei pasinaudoti teisių gynimo priemone.</td></tr>
<tr><td colspan="2">10. Gavus duomenų subjekto kreipimąsi dėl jo asmens duomenų neteisingumo, neišsamumo, netikslumo Kolegijos atsakingas asmuo nedelsdamas patikrina asmens duomenis ir duomenų subjekto rašytiniu prašymu, pateiktu asmeniškai, paštu ar elektroninių ryšių priemonėmis, patikrinus / įsitikinus Duomenų subjekto tapatybę ir Asmens duomenis patvirtinančių dokumentų atitiktį / atitiktimi teisės aktų reikalavimams, nedelsdamas privalo ištaisyti neteisingus, neišsamius, netikslius Asmens duomenis arba sustabdo tokių duomenų tvarkymo veiksmus, išskyrus saugojimą.</td></tr>
<tr><td colspan="2">11. Gavus duomenų subjekto kreipimąsi dėl jo duomenų tvarkymo neteisėtumo, nesąžiningumo Kolegijos atsakingas asmuo nedelsdamas patikrina duomenų tvarkymo teisėtumą, nesąžiningumą ir, gavus rašytinį prašymą, patikrinus / įsitikinus asmens dokumentų atitiktį / atitiktimi teisės aktų reikalavimams, nedelsdamas sunaikina neteisėtai ir nesąžiningai sukauptus asmens duomenis ar sustabdo tokių duomenų tvarkymo veiksmus, išskyrus saugojimą.</td></tr>
</table>

XII SKYRIUS
POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS (PDAV) IR IŠANKSTINĖS KONSULTACIJOS SU PRIEŽIŪROS INSTITUCIJA

<table>
<tr><td colspan="2">1. Poveikio duomenų apsaugai vertinimas (PDAV) – tai procesas, kurio metu vertinamas pavojus fizinių asmenų teisėms ir laisvėms, vertinant netinkamo duomenų valdymo ir jų praradimo įvykio tikimybę ir galimas pasekmes.</td></tr>
<tr><td colspan="2">2. Pavojaus vertinimo tikslas yra nustatyti ir įvertinti esamą ar galimą pavojų, susijusį su vertinamu procesu, jį pašalinti, o jei negalima pašalinti, taikyti prevencijos priemones, kad vertinamas procesas būtų apsaugotas nuo pavojaus arba jis būtų kiek įmanoma sumažintas.</td></tr>
<tr><td>3. Kolegijai pradėjus vykdyti naują (-as) duomenų tvarkymo operaciją (-as), yra privaloma atlikti PDAV, jei duomenų tvarkymas:</td><td>3.1. keltų didelį pavojų duomenų subjektų teisėms ir laisvėms (pavyzdžiui, atvejai, kai duomenų subjektas neturi galimybės nesutikti su duomenų tvarkymu, duomenys perduodami už ES ribų, būtų pradėti tvarkyti duomenys, kurie gauti juos sujungus su duomenimis iš kitų šaltinių, būtų tvarkomi jautrūs duomenys, tokie kaip sveikata, būtų pradėti naudoti nauji technologiniai sprendimai, pavyzdžiui, veido atpažinimo sistemos, ar kitų biometrinių duomenų atpažinimo ir kt.);
3.2. automatizuotai būtų tvarkomi asmeniniai aspektai, vykdomas profiliavimas ir priimami teisiniai ar kiti didelio poveikio (pavyzdžiui, asmenų suskirstymas į grupes, kuris gali turėti jiems įtakos) sprendimai;
3.3. būtų pradėtas vykdyti sistemingas vaizdo stebėjimas dideliu mastu;
3.4. būtų pradėti tvarkyti specialių kategorijų asmens duomenys dideliu mastu.</td></tr>
<tr><td colspan="2">4. PDAV taip pat gali būti atliekamas ir šiame skyriuje neaptartais atvejais, bet esant Kolegijos vadovo sprendimu tai atlikti.</td></tr>
<tr><td colspan="2">5. PDAV atlieka Kolegijos vadovo įsakymu sudaroma darbo grupė iš Kolegijos darbuotojų arba PDAV atlieka asmenys pagal paslaugų teikimo sutartį.</td></tr>
<tr><td colspan="2">6. Kolegijos vadovo įsakymu sudaromai darbo grupei paskiriamas jos vadovas atlikti PDAV. Į jos sudėtį gali būti įtrauktas ir Pareigūnas arba gali būti konsultuojamasi su Pareigūnu.</td></tr>
<tr><td colspan="2">7. Darbo grupė PDAV metu pildo Priežiūros institucijos rekomenduojamą PDAV formą (toliau – Forma).</td></tr>
<tr><td colspan="2">8. Užpildyta ir pasirašyta Forma teikiama Kolegijos vadovui, kuris priima sprendimus dėl tolimesnio asmens duomenų tvarkymo.</td></tr>
<tr><td colspan="2">9. Kai iš PDAV paaiškėja, kad duomenų tvarkymo operacijos kelia didelį pavojų duomenų subjektų teisėms ir laisvėms, o Kolegija negali jo sumažinti tinkamomis rizikos valdymo priemonėmis (turimomis technologijomis ir įgyvendinimo sąnaudomis), prieš pradedant asmens duomenų tvarkymą turi būti iš anksto konsultuojamasi su Priežiūros institucija.</td></tr>
<tr><td colspan="2">10. Konsultavimasis su Priežiūros institucija atliekamas pagal Priežiūros institucijos nustatytą procedūrą ir reikalavimus.</td></tr>
</table>

XIII SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMAS

1. Pažeidimai pagal pobūdį (tipą):	1.1. konfidencialumo pažeidimas – neleistinas arba netyčinis asmens duomenų atskleidimas arba prieigos prie jų suteikimas (pavyzdžiui, atskleisti duomenys ir jie tapo prieinami tretiesiems asmenims, suteikiant prieigą, tinkamai nešifruojant, kt.); 1.2. duomenų pasiekiamumo / prieinamumo – neleistinas arba netyčinis prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas (pavyzdžiui, prarasti duomenys ir neturima atsarginių kopijų); 1.3. duomenų vientisumo pažeidimas – neleistinas arba netyčinis asmens duomenų pakeitimas (pavyzdžiui, prarasti studentų duomenys, turima tik dalis atsarginių kopijų, dėl ko neįmanoma „atkurti“ visos su mokiniu bendravimo istorijos); 1.4. mišraus pobūdžio (tipo) pažeidimas – asmens duomenų konfidencialumo, prieinamumo ir vientisumo pažeidimas ar bet kurių aukščiau nurodytų pažeidimų derinys. 1.5. Pažeidimus gali nustatyti / informaciją apie pažeidimus gali gauti bet kuris Kolegijos darbuotojas.
2. Pažeidimas gali įvykti dėl šių priežasčių:	2.1. žmogiškoji klaida (pvz., asmens duomenys persiųsti ne tam adresatui, kuriam jie buvo skirti; ne saugojimui skirtoje vietoje palikti dokumentai, kuriuose yra asmens duomenų; pamesti nešiojami / mobilūs įrenginiai (telefonas, nešiojamas kompiuteris, išorinės duomenų laikmenos), kuriuose saugomi asmens duomenys ir kt.); 2.2. vagystė (pvz., pavogti nešiojami / mobilūs įrenginiai, kuriuose saugomi asmens duomenys; pavogtos neautomatiniu būdu susistemintos bylos, kuriose yra asmens duomenų ir kt.); 2.3. kibernetinė ataka (pvz., duomenų bazėje ar informacinėje sistemoje esantys asmens duomenys užšifruojami, naudojant išpirkos reikalaujančią programą; internete paskelbiami informacinių sistemų naudotojų vardai ir slaptažodžiai ir kt.); 2.4. įrenginių ar programinės įrangos gedimas, saugos sistemos spragos (pvz., energijos tiekimo nutrūkimas, dėl kurio negalima prieiga prie asmens duomenų; programos kodo, kuriuo kontroliuojamas prieigos teisių suteikimas informacinių sistemų naudotojams, klaida ir kt.); 2.5. nenumatytos (force majeure) aplinkybės ir kitos priežastys (gaisras, vandens užliejimas, dėl kurių sugadinami arba prarandami asmens duomenys ir kt.).
3. Pažeidimų valdymas	3.1. Kolegijos darbuotojas, pastebėjęs, nustatęs, gavęs informaciją apie galimą Pažeidimą iš duomenų tvarkytojo ar kito šaltinio, privalo: 3.1.1. nedelsiant, bet ne vėliau kaip per 2 darbo valandas nuo galimo Pažeidimo paaiškėjimo momento informuoti žodžiu, raštu ar elektroninėmis priemonėmis Kolegijos vadovo įgaliotą darbuotoją ir Pareigūną); 3.1.2. užpildyti pranešimą apie asmens duomenų saugumo pažeidimą (Taisyklių priedas Nr. 3) ir nedelsiant, bet ne vėliau kaip per 4 darbo valandas nuo galimo pažeidimo paaiškėjimo momento perduoti jį Kolegijos vadovo įgaliotam darbuotojui, o jo

	kopiją – Pareigūnui; 3.1.3. jei įmanoma, imtis priemonių pašalinti galimą Pažeidimą ir imtis priemonių galimoms neigiamoms jo pasekmėms sumažinti.
4. Kolegijos vadovo įgaliotas darbuotojas, gavęs pranešimą apie ažeidimą, privalo:	4.1. atlikti pažeidimo tyrimą ir nedelsdamas, bet ne vėliau kaip per 24 valandas nuo pranešimo gavimo momento nagrinėti pranešime nurodytas aplinkybes; 4.2. įvertinti, ar padarytas pažeidimas; 4.3. konsultuotis su Pareigūnu; 4.4. jei pažeidimas yra susijęs su elektroninės informacijos saugos incidentu, pasitelkti Kolegijos ar duomenų tvarkytojo IT specialistus; 4.5. jei pažeidimas padarytas, nustatyti, kokio pobūdžio (tipo) pažeidimas padarytas, asmens duomenų, kurių saugumas pažeistas, kategorijas, įskaitant specialių kategorijų asmens duomenis, pažeidimo priežastis, pažeidimo apimtis, esamas ir (ar) galimas pasekmes ir žalą, padarytą duomenų subjektui (-ams), įvertinti pavojų duomenų subjekto teisėms ir laisvėms (toliau – rizika), kuris gali atsirasti dėl galimo pažeidimo, pateikti užpildytą Pareigūnui Asmens duomenų saugumo pažeidimo tyrimo ataskaitą (Taisyklių priedas Nr. 4) dėl pažeidimo buvimo ir rizikos; 4.6. teikti rekomendacijas Kolegijos darbuotojams, atsakingiems už pažeidimo ir (ar) jo pasekmių pašalinimą ir (ar) sumažinimą, ir (ar) duomenų tvarkytojui dėl tinkamų techninių ir organizacinių priemonių, kad pažeidimas būtų išsamiai ištirtas ir jis ir (ar) jo pasekmės būtų pašalintos ir (ar) sumažintos ir pažeidimas ateityje nepasikartotų, taikymo ir (arba) pats imtis šių veiksmų; 4.7. įvertinti, kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas pažeidimas; 4.8. nustatyti, ar apie pažeidimą būtina pranešti VDAI; 4.9. nustatyti, ar apie pažeidimą būtina pranešti duomenų subjektams.
5. Pareigūnas, gavęs pranešimą privalo:	5.1. Kolegijos vadovo įgaliotam asmeniui patarti dėl Pažeidimo tyrimo ir teikti išvadas dėl Pranešimo teikimo VDAI ir (ar) duomenų subjektui; 5.2. bendradarbiauti su VDAI dėl pažeidimų; 5.3. stebėti, kaip vykdomos BDAR ir Taisyklėse nustatytos Kolegijos pareigos, susijusios su pažeidimų valdymu.
6. Tyrimo metu nustačius, kad pažeidimas buvo, Kolegijos vadovui priėmus sprendimą dėl Pranešimo priežiūros institucijai pateikimo būtinybės, Kolegijos vadovo įgaliotas darbuotojas privalo **nedelsiant, bet ne vėliau nei kaip per 72 val.** nuo tada, kai tapo žinoma apie pažeidimą, apie tai informuoti VDAI, išskyrus atvejus, kai pažeidimas nekelia pavojaus fizinių asmenų teisėms ir laisvėms. Jeigu įvertinus riziką, abejojama, ar Pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, apie pažeidimą pranešama VDAI.	
7. VDAI informuojama pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo, patvirtinto VDAI direktoriaus 2018 m. liepos 27 d. įsakymu Nr. 1T-72(1.12.E) „Dėl pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo patvirtinimo“ (su visais aktualiais pakeitimais), nustatyta tvarka ir sąlygomis, užpildant pranešimo apie asmens duomenų saugumo pažeidimo formą, patvirtintą VDAI direktoriaus 2018 m. rugpjūčio 29 d. įsakymu Nr. 1T-82(1.12.E) „Dėl pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo“ (Taisyklių priedas Nr. 5).	

8. Jeigu įvertinus riziką, nustatoma, kad tuo metu apie pažeidimą VDAI pranešti nereikia, po kurio laiko situacija gali pasikeisti, todėl pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo.
9. Tyrimo metu nustačius, kad dėl pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, Kolegijos vadovo įgaliotas darbuotojas nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo to laiko, kai buvo sužinota apie pažeidimą, praneša apie tai duomenų subjektui, kurio teisėms ir laisvėms gali kilti didelis pavojus. Pagrindinis pranešimo duomenų subjektui tikslas – pateikti konkrečią informaciją apie tai, kokių veiksmų jis turėtų imtis, kad apsisaugotų nuo neigiamų pažeidimo pasekmių. Tam tikromis aplinkybėmis, kai tai yra pagrįsta, Kolegija pasitarusi su teisėsaugos institucijomis ir atsižvelgdama į teisėtus teisėsaugos interesus, gali atidėti asmenų, kuriems pažeidimas turi poveikio, informavimą apie saugumo pažeidimą iki to laiko, kai tai netrukdys saugumo pažeidimo tyrimams.
10. Visi pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI ir (ar) duomenų subjektui, ar tokie pažeidimai kelia riziką, registruojami Asmens duomenų saugumo pažeidimų registravimo žurnale (Taisyklių priedas Nr. 6). Už žurnalo pildymą ir saugojimą atsakingas Kolegijos Pareigūnas. Žurnalas gali būti popierinės arba elektroninės formos. Užpildytas žurnalas saugomas 5 metus nuo paskutinio įrašo žurnale padarymo dienos. Žurnalas yra pateikiamas VDAI jai pareikalavus.
11. Pareigūnas ar kitas Kolegijos vadovo įgaliotas darbuotojas privalo užtikrinti, kad visos neatitiktys, įskaitant ir asmens duomenų apsaugos incidentus būtų tinkamai dokumentuotos ir saugomos.

XIV SKYRIUS
ASMENS DUOMENŲ APSAUGOS PAREIGŪNAS

1. Kolegijos vadovo įsakymu, Pareigūnas gali būti paskirtas iš esamų Kolegijos darbuotojų, naujas darbuotojas arba asmuo, su kuriuo būtų sudaroma paslaugų teikimo sutartis.	
2. Kolegijos vadovas paskyręs arba sudaręs su Pareigūnu paslaugų teikimo sutartį, privalo užtikrinti, kad Pareigūno kontaktiniai duomenys per protingą terminą nuo jo paskyrimo / paslaugų sutarties sudarymo būtų tinkamai paskelbti duomenų subjektams bei pranešti VDAI.	
3. Skirdamas Pareigūną, Kolegijos vadovas privalo įvertinti ir įgyvendinti tai, kad:	3.1. Pareigūnas turėtų tinkamų asmens duomenų teisinės apsaugos praktinių ir ekspertinių žinių; 3.2. Pareigūnas būtų įtraukiamas į visų su asmens duomenų apsauga ir privatumu susijusių klausimų nagrinėjimą Kolegijoje; 3.3. Pareigūnas būtų tiesiogiai pavaldus Kolegijos vadovui; 3.4. Pareigūnas neturėtų jokių kitų pareigų, neatliktų funkcijų, kurios galėtų sukelti interesų konfliktą su jo atliekamomis Pareigūno funkcijomis.
4. Pareigūnas privalo:	4.1. užtikrinti, kad Kolegijoje vykdomas asmens duomenų tvarkymas atitiktų BDAR, kitų, asmens duomenų teisinę apsaugą reglamentuojančių teisės aktų reikalavimus, tinkamai įvertinant duomenų tvarkymo operacijas, duomenų tvarkymo pobūdį, aprėptį, kontekstą, tikslus, potencialų pavojų; 4.2. stebėti, kaip laikomasi BDAR, kitų, asmens duomenų teisinę apsaugą reglamentuojančių teisės aktų reikalavimų, šių Taisyklių, kitų vidinių dokumentų, susijusių su asmens duomenų apsauga; 4.3. konsultuoti ir stebėti, kaip Kolegijoje atliekamas poveikio duomenų apsaugai vertinimas; 4.4. informuoti Kolegijos vadovą ir kitus darbuotojus apie jų pareigas pagal BDAR ir kitus, asmens duomenų teisinę apsaugą reglamentuojančius, teisės aktus ir juos konsultuoti dėl konkrečių pareigų vykdymo; 4.5. informuoti Kolegijos vadovą apie bet kokius neatitikimus, pažeidimus asmens duomenų apsaugos srityje, kuriuos Pareigūnas nustato, vykdydamas savo funkcijas; 4.6. mokyti Kolegijos darbuotojus, dirbančius su asmens duomenimis, asmens duomenų teisinės apsaugos klausimais; 4.7. bendradarbiauti, būti kontaktiniu asmeniu santykiuose su VDAI; 4.8. atlikti kitas, su asmens duomenų tvarkymu ir apsauga susijusias funkcijas, numatytas paslaugų teikimo sutartyje (jei Pareigūno paslauga perkama) ir/ar Kolegijos vidaus teisės aktuose.
5. Pareigūnas savo pareigas ir užduotis atlieka nepriklausomai. Kolegijos vadovas, ir jokie kiti Kolegijos darbuotojai Pareigūnui negali teikti jokių nurodymų dėl jo užduočių vykdymo.	
6. Pareigūnas turi teisę naudotis Kolegijos teisės, personalo, informacinių technologijų, kitų padalinių pagalba, prašyti ir gauti iš jų informaciją, reikalingą jo funkcijoms vykdyti.	

XV SKYRIUS
BAIGIAMOSIOS NUOSTATOS

1. Darbuotojai privalo laikytis Taisyklėse nustatytų įpareigojimų bei atlikdami savo darbo funkcijas vadovautis jose nustatytais principais. Priėmus naują darbuotoją, jis su Taisyklėmis privalo būti supažindintas pirmąją jo darbo dieną.
2. Darbuotojai su Taisyklėmis bei jos pakeitimais supažindinami pasirašytinai arba išsiunčiant jiems sukurtu Kolegijos elektroniniu paštu ar pateikiant informaciją naudojantis kitomis informacinėmis technologinėmis priemonėmis.
3. Šiose Taisyklėse esančios nuostatos gali būti papildomos ar išsamiau įtvirtinamos kituose Kolegijos veiklą reguliuojančiuose vidaus dokumentuose. Rengiant vidaus dokumentus, visais atvejais turi būti vadovaujamasi Taisyklėmis. Jeigu duomenų apsaugos klausimais yra prieštaravimų tarp Taisyklių ir kitų Kolegijos vidaus dokumentų, turi būti vadovaujamasi Taisyklių nuostatomis. Tuo atveju, jeigu klausimai, susiję su asmens duomenų apsauga nėra reglamentuoti Taisyklėse, turi būti taikomi kiti Kolegijos vidaus dokumentai.
4. Apie šias Taisykles yra informuota Kolegijos darbo taryba ir dėl jų priėmimo su ja konsultuotasi.
5. Kolegijos darbuotojai, pažeidę Taisykles, ADTAĮ ir (ar) BDAR, atsako teisės aktų nustatyta tvarka.
6. Pasikeitus asmens duomenų tvarkymą reglamentuojantiems teisės aktams, Taisyklės yra peržiūrimos ir atnaujinamos.
7. Šios Taisyklės tvirtinamos, keičiamos Kolegijos direktoriaus įsakymu.
8. Taisyklių priedai, jeigu tokių yra, tampa neatsiejama šių Taisyklių dalimi.

Asmens duomenų
tvarkymo taisyklių
1 priedas

MARIJAMPOLĖS KOLEGIJOS ASMENS DUOMENŲ TVARKYMO REGISTRAVIMO ŽURNALAS

EIL. NR.	DUOMENŲ SUBJEKTO VARDAS, PAVARDĖ	KONTAKTAI	KREIPIMOSI DATA	PRAŠYMO TIPAS	PASTABOS (KAS ATLIKTA)	DUOMENŲ VALDYTOJO ĮGALIOTAS ASMUO	ATSAKYMO PATEIKIMO DATA

Asmens duomenų
tvarkymo taisyklių
2 priedas

PRAŠYMO ĮGYVENDINTI DUOMENŲ SUBJEKTO TEISĘ (-ES) REKOMENDUOJAMA FORMA

_____

Duomenų subjekto (fizinio asmens) vardas, pavardė

_____

(Kontaktinė informacija: gyvenamoji vieta, telefono numeris, elektroninio pašto adresas (nurodoma duomenų subjektui pageidaujant)

arba atstovas ir atstovavimo pagrindas, jeigu prašymą pateikia duomenų subjekto atstovas)

Kolegijos vadovui

PRAŠYMAS
DĖL DUOMENŲ SUBJEKTO TEISIŲ (-ĖS) ĮGYVENDINIMO
20 m. d.

_____
(prašymo sudarymo vieta)

Prašau įgyvendinti šią (šias) duomenų subjekto teisę (-es)*:

*Tinkamą langelį pažymėkite kryželiu

☐ **Teisė gauti informaciją apie duomenų tvarkymą.**
☐ **Teisė susipažinti su tvarkomais duomenimis.**
☐ **Teisė reikalauti ištaisyti duomenis.**
☐ **Teisė reikalauti ištrinti duomenis („Teisė būti pamirštam“).** Ši teisė netaikoma, jei asmens duomenys, kuriuos prašoma ištrinti, yra tvarkomi ir kitu teisiniu pagrindu, tokiu kaip tvarkymas būtinas sutarties vykdymui arba yra pareigos pagal taikomus teisės aktus vykdymas.
☐ **Teisė apriboti duomenų tvarkymą.**
☐ **Teisė nesutikti su duomenų tvarkymu.**
☐ **Teisė į duomenų perkeliamumą.** Teisė į duomenų perkeliamumą negali daryti neigiamo poveikio kitų teisėms ir laisvėms. Duomenų subjektas teisės į duomenų perkeliamumą neturi tų asmens duomenų atžvilgiu, kurie tvarkomi neautomatiniu būdu susistemintose rinkmenose, pavyzdžiui, popierinėse bylose.
☐ **Teisė reikalauti, kad nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas.**

Kita informacija**:

** Nurodykite, ko konkrečiai prašote ir pateikite kiek įmanoma daugiau informacijos, kuri leistų tinkamai įgyvendinti Jūsų teisę (-es) *(pavyzdžiui, jeigu norite gauti asmens duomenų kopiją, nurodykite, kokių konkrečiai duomenų (pavyzdžiui, 2018 m. x mėn. x d. elektroninio pašto laiško kopiją, 2018 m. x mėn. x d. vaizdo įrašą (x val. x min. – x val. x min.) kopiją pageidaujate gauti; jeigu norite ištaisyti duomenis, nurodykite, kokie konkrečiai Jūsų asmens duomenys yra netikslūs; jeigu nesutinkate, kad būtų tvarkomi Jūsų asmens duomenys, tuomet nurodykite argumentus, kuriais grindžiate savo nesutikimą, nurodykite dėl kokio konkrečiai duomenų tvarkymo nesutinkate; jeigu kreipiatės dėl teisės į duomenų perkeliamumą įgyvendinimo, prašome nurodyti, kokių duomenų atžvilgiu šią teisę pageidaujate įgyvendinti, ar pageidaujate juos perkelti į savo įrenginį ar kitam duomenų valdytojui, jeigu pastarajam, tuomet nurodykite kokiam):*

_____
_____
_____
_____

PRIDEDAMA***:

*** Jeigu prašymas yra siunčiamas paštu, prie prašymo pridedama asmens tapatybę patvirtinančio dokumento kopija, patvirtinta notaro ar kita teisės aktų nustatyta tvarka. Jeigu kreipiamasi dėl netikslių duomenų ištaisymo, pateikiamos tikslius duomenis patvirtinančių dokumentų kopijas; jeigu jos siunčiamos paštu, tuomet turi būti patvirtintos notaro ar kita teisės aktų nustatyta tvarka. Jeigu duomenų subjekto asmens duomenys, tokie kaip vardas, pavardė, yra pasikeitę, kartu pateikiamos dokumentų, patvirtinančių šių duomenų pasikeitimą, kopijos; jeigu jos siunčiamos paštu, tuomet turi būti patvirtintos notaro ar kita teisės aktų nustatyta tvarka.

(parašas) *(Vardas Pavardė)*

Asmens duomenų
tvarkymo taisyklių
3 priedas

(Pranešimo apie asmens duomenų saugumo pažeidimą forma įstaigos viduje)

_____
(juridinio asmens pavadinimas)

_____
(struktūrinio padalinio pavadinimas)

_____
(pareigų pavadinimas)

_____
(vardas, pavardė)

PRANEŠIMAS
APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____ Nr. _____
(data, dokumento numeris)

_____
(miestas)

Informuoju apie asmens duomenų saugumo pažeidimą, pateikdamas turimą informaciją:
1. Asmens duomenų saugumo pažeidimo nustatymo data, laikas ir vieta:

2. Asmens duomenų saugumo pažeidimo padarymo data, laikas ir vieta:

3. Asmens duomenų saugumo pažeidimo esmė ir aplinkybės:

4. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (pvz., įstaigos darbuotojai, asmenys, pateikę prašymus, skundus, asmenys, užsisakę įstaigos naujienlaiškius ir kt.) ir apytikslis jų skaičius:

5. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-us):

☐ Asmens tapatybę patvirtinantys duomenys (vardas, pavardė, gimimo data, lytis ir kt.)

☐ Asmens identifikaciniai ar prisijungimo duomenys (asmens kodas, mokėtojo kodas, slaptažodžiai ir kt.)

☐ Asmens kontaktiniai duomenys (gyvenamosios vietos adresas, telefono numeris, elektroninio pašto adresas ir kt.)

☐ Specialių kategorijų asmens duomenys (duomenys, susiję su asmens sveikata, genetiniai duomenys, biometriniai duomenys, duomenys, susiję su asmens rasine ar etnine kilme, duomenys, susiję su asmens politinėmis pažiūromis, religiniais, filosofiniais įsitikinimais ar naryste profesinėse sąjungose, duomenys susiję su asmens lytiniu gyvenimu ir lytine orientacija ir kt.)

☐ Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas

☐ Kiti asmens duomenys (įrašyti):

6. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius:

7. Kokių veiksmų (priemonių) buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą (pvz., pakeisti prisijungimo prie informacinės sistemos slaptažodžiai, panaudotos atsarginės kopijos, siekiant atkurti prarastus ar sugadintus duomenis, atnaujinta programinė įranga, surinkti ne saugojimui skirtoje vietoje palikti dokumentai su asmens duomenimis ir kt.):

_____	_____	_____
(pareigos)	(parašas)	(vardas ir pavardė)

Asmens duomenų
tvarktmo taisyklių
4 priedas

(Asmens duomenų saugumo pažeidimo tyrimo ataskaitos forma)

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMO ATASKAITA

_____ Nr. _____
(data, dokumento numeris)

1. Asmens duomenų saugumo pažeidimo aprašymas

1.1. Asmens duomenų saugumo pažeidimo data ir laikas:

Asmens duomenų saugumo pažeidimo data ☐ laikas

Asmens duomenų saugumo pažeidimo nustatymo data ☐ laikas

1.2. Asmens duomenų saugumo pažeidimo vieta (pažymėti tinkamą (-us):

☐ Informacinė sistema

☐ Duomenų bazė

☐ Tarnybinė stotis

☐ Internetinė svetainė

☐ Debesų kompiuterijos paslaugos

☐ Nešiojami / mobilūs įrenginiai

☐ Neautomatiniu būdu susistemintos bylos (archyvas)

☐ Kita (įrašyti):

1.3. Asmens duomenų saugumo pažeidimo pobūdis (pažymėti tinkamą (-us):

☐ Konfidencialumo pažeidimas (neautorizuota prieiga ar atskleidimas)

☐ Vientisumo pažeidimas (neautorizuotas asmens duomenų pakeitimas)

☐ Prieinamumo pažeidimas (asmens duomenų praradimas, sunaikinimas)

1.4. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-us) ir aprašyti):

☐ Asmens tapatybę patvirtinantys duomenys (vardas, pavardė, gimimo data, lytis ir kt.):

☐ Asmens identifikaciniai ar prisijungimo duomenys (asmens kodas, mokėtojo kodas, slaptažodžiai ir kt.):

☐ Asmens kontaktiniai duomenys (gyvenamosios vietos adresas, telefono numeris, elektroninio pašto adresas ir kt.):

☐ Specialių kategorijų asmens duomenys (duomenys, susiję su asmens sveikata, genetiniai duomenys, biometriniai duomenys, duomenys, susiję su asmens rasine ar etnine kilme, duomenys,

susiję su asmens politinėmis pažiūromis, religiniais, filosofiniais įsitikinimais ar naryste profesinėse sąjungose, duomenys susiję su asmens lytiniu gyvenimu ir lytine orientacija ir kt.):

☐ Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:

☐ Kiti asmens duomenys:

1.5. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius:

1.6. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (Administracijos darbuotojai, asmenys, pateikę prašymus, skundus, asmenys, užsisakę Savivaldybės naujienlaiškius ir kt.):

1.7. Apytikslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius:

1.8. Darbuotojas, pranešęs apie asmens duomenų saugumo pažeidimą (vardas, pavardė, Administracijos struktūrinio padalinio, kuriame dirba darbuotojas, pavadinimas, telefono numeris, elektroninio pašto adresas):

1.9. Duomenų tvarkytojas, pranešęs apie asmens duomenų saugumo pažeidimą (pavadinimas, kontaktinio asmens duomenys (vardas, pavardė, telefono numeris, elektroninio pašto adresas):

---

2. Asmens duomenų saugumo pažeidimo keliamos rizikos duomenų subjektų teisėms ir laisvėms įvertinimas

2.1. Specifiniai fizinių asmenų, kurių asmens duomenų saugumas buvo pažeistas, ypatumai (vaikai, asmenys su negalia ir kt.):

2.2. Galimybė identifikuoti fizinį asmenį (pvz., iki asmens duomenų saugumo pažeidimo asmens duomenys buvo tinkamai užšifruoti, anonimizuoti, arba iki saugumo pažeidimo asmens duomenims šifravimas nebuvo taikomas ir kt.):

2.3. Kas gavo prieigą prie asmens duomenų, kurių saugumas pažeistas?

2.4. Ar buvo kokių kitų įvykių ar aplinkybių, turėjusių poveikį asmens duomenų saugumo pažeidimo padarymui?

2.5. Kokia žala padaryta fiziniams asmenims (duomenų subjektams)?

2.6. Galimos asmens duomenų saugumo pažeidimo pasekmės:

2.6.1. Konfidencialumo pažeidimo atveju (pažymėti tinkamą (-us):

☐ Asmens duomenų išplitimas ir duomenų subjekto kontrolės praradimas savo asmens duomenų atžvilgiu (pvz., asmens duomenys išplito internete)

☐ Skirtingos informacijos susiejimas (pvz., gyvenamosios vietos adreso susiejimas su asmens buvimo vieta realiu laiku)

☐ Galimas panaudojimas kitais, nei nustatytais ar neteisėtais tikslais (pvz., komerciniais tikslais, asmens tapatybės pasisavinimo tikslu, informacijos panaudojimo prieš asmenį tikslu)

☐ Kita:

2.6.2. Vientisumo pažeidimo atveju (pažymėti tinkamą (-us):

☐ Pakeitimas į neteisingus duomenis, dėl ko asmuo gali netekti galimybės naudotis paslaugomis

☐ Pakeitimas į kitus duomenis, kad asmens duomenų tvarkymas būtų nukreiptas tam tikra linkme (pvz., pavogta asmens tapatybė susiejant vieno asmens identifikuojančius duomenis su kito asmens biometriniais duomenimis)

☐ Kita:

2.6.3. Prieinamumo pažeidimo atveju (pažymėti tinkamą (-us):

☐ Dėl asmens duomenų trūkumo negalima teikti paslaugų (pvz., administracinių procesų sutrikdymas, dėl ko negalima prieiti prie tvarkomų asmens duomenų ir įgyvendinti duomenų subjekto teisę susipažinti su jo tvarkomais asmens duomenimis)

☐ Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamos paslaugos (pvz., tam tikra informacija iš informacinės sistemos išnyko, dėl ko negalima tinkamai suteikti administracinės paslaugos)

☐ Kita:

2.7. Asmens duomenų saugumo pažeidimo sukeltos rizikos duomenų subjektų teisėms ir laisvėms lygis:

☐ Žema rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo nėra pavojaus fizinių asmenų teisėms ir laisvėms)

☐ Vidutinė rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo yra / gali kilti pavojus fizinių asmenų teisėms ir laisvėms)

☐ Didelė rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo yra / gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms)

2.8. Kokių veiksmų / priemonių buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą?

2.9. Kokios taikytos priemonės, siekiant sumažinti neigiamą poveikį duomenų subjektams?

2.10. Kokios techninės priemonės buvo taikomos asmens duomenų saugumo pažeidimo paveiktiems asmens duomenims, užtikrinant, kad asmens duomenys nebūtų prieinami neįgaliotiems asmenims?

2.11. Techninės ir / ar organizacinės saugumo priemonės, kurios įgyvendintos dėl asmens duomenų saugumo pažeidimo, taip pat siekiant, kad pažeidimas nepasikartotų:

2.12. Techninės ir / ar organizacinės saugumo priemonės, kurios ketinamos įgyvendinti dėl asmens duomenų saugumo pažeidimo, įskaitant ir priemones sumažinti asmens duomenų saugumo pažeidimo pasekmes:

3. Pranešimų apie asmens duomenų saugumo pažeidimą pateikimas

3.1. Ar pranešta Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI) apie asmens duomenų saugumo pažeidimą?

☐ Taip

Pranešimo VDAI data [ ] numeris

☐ Ne (nurodomos nepranešimo VDAI priežastys):

☐ Apie duomenų saugumo pažeidimą pranešta VDAI vėliau nei per 72 valandas (nurodomos vėlavimo pranešti VDAI priežastys):

3.2. Ar pranešta duomenų subjektui apie asmens duomenų saugumo pažeidimą?

☐ Taip

Pranešimo duomenų subjektui data [ ] numeris (jeigu pranešimas užregistruotas)

Pranešimo duomenų subjektui būdas (pažymėti tinkamą (-us): ☐ paštu ☐ elektroniniu paštu ☐ trumpąja žinute (SMS) ☐ kitais būdais

Informuotų duomenų subjektų skaičius

Pranešimo duomenų subjektui turinys:

☐ Ne (nurodomos nepranešimo duomenų subjektui priežastys):

☐ Apie duomenų saugumo pažeidimą duomenų subjektams pranešta vėliau nei per 72 valandas (nurodomos vėlavimo pranešti duomenų subjektui priežastys):

☐ Apie saugumo pažeidimą pranešta viešai (nurodoma kada ir kur paskelbta informacija viešai arba jei taikyta kita priemonė, nurodoma kokia ir kada taikyta):

3.3. Ar pranešta valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, apie asmens duomenų saugumo pažeidimą, galimai turintį nusikalstamos veikos požymių (jeigu taip, nurodoma rašto data ir numeris):

Atsakingas asmuo:

_____ _____ _____

(pareigos) (parašas) (vardas ir pavardė)

Susipažino duomenų apsaugos pareigūnas:

_____ _____

(parašas) (vardas ir pavardė)

Asmens duomenų
tvarkymo taisyklių
5 priedas

_____

(duomenų valdytojo (juridinio asmens) pavadinimas, duomenų valdytojo atstovo pavadinimas, duomenų valdytojo (fizinio asmens) vardas, pavardė)

_____

(juridinio asmens kodas ir buveinės adresas arba fizinio asmens kodas, gimimo data (jeigu asmuo neturi asmens kodo) ir asmens duomenų tvarkymo vieta

_____

(telefono ryšio ir (ar) elektroninio pašto adresas, ir (ar) elektroninės siuntos pristatymo dėžutės adresas)

Valstybinei duomenų apsaugos inspekcijai

PRANEŠIMAS
APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____Nr. _____
(data) (rašto numeris)

1. Asmens duomenų saugumo pažeidimo apibūdinimas

1.1. Asmens duomenų saugumo pažeidimo data ir laikas:

Asmens duomenų saugumo pažeidimo :

Data _____ Laikas _____

Asmens duomenų saugumo pažeidimo nustatymo:

Data _____ Laikas _____

1.2. Asmens duomenų saugumo pažeidimo vieta (pažymėti tinkamą (-us):

11.1.

- Informacinė sistema
- Duomenų bazė
- Tarnybinė stotis
- Internetinė svetainė
- Debesų kompiuterijos paslaugos
- Nešiojami / mobilūs įrenginiai
- Neautomatiniu būdu susistemintos bylos (archyvas)
- Kita _____

11.2.
11.3.
11.4.

1.3. Asmens duomenų saugumo pažeidimo aplinkybės (pažymėti tinkamą (-us):

- Asmens duomenų konfidencialumo praradimas (neautorizuota prieiga ar atskleidimas)
- Asmens duomenų vientisumo praradimas (neautorizuotas asmens duomenų pakeitimas)
- Asmens duomenų prieinamumo praradimas (asmens duomenų praradimas, sunaikinimas)

11.5.

1.4. Apytikslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius:

_____

11.6.

1.5. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (atskiriamos pagal jai būdingą požymį):

_____
_____

1.6. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-as):

☐ Asmens tapatybę patvirtinantys asmens duomenys (vardas, pavardė, amžius, gimimo data, lytis ir kt.):

_____
_____

11.7.

☐ Specialių kategorijų asmens duomenys (duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, ar narystę profesinėse sąjungose, genetiniai duomenys, biometriniai duomenys, sveikatos duomenys, duomenys apie lytinį gyvenimą ir lytinę orientaciją):

_____
_____
_____

11.8.

☐ Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:

11.9. _____
_____

☐ Prisijungimo duomenys ir (ar) asmens identifikaciniai numeriai (pavyzdžiui, asmens kodas, mokėtojo kodas, slaptažodžiai):

_____
_____

11.10.

☐ Kiti:

_____
_____

11.11.

☐ Nežinomi (pranešimo teikimo metu)

11.12.

1.7. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius:

_____

1.8. Kita duomenų valdytojo nuomone reikšminga informacija apie asmens duomenų saugumo pažeidimą:

_____
_____
_____
_____
_____

2. Galimos asmens duomenų saugumo pažeidimo pasekmės

2.1. Konfidencialumo praradimo atveju:

11.13.

- Asmens duomenų išplitimas labiau nei yra būtina ir duomenų subjekto kontrolės praradimas savo asmens duomenų atžvilgiu (pavyzdžiui, asmens duomenys išplito internete)
- Skirtingos informacijos susiejimas (pavyzdžiui, gyvenamosios vietos adreso susiejimas su asmens buvimo vieta realiu laiku)
- Galimas panaudojimas kitais, nei nustatytais ar neteisėtais tikslais (pavyzdžiui, komerciniais tikslais, asmens tapatybės pasisavinimo tikslu, informacijos panaudojimo prieš asmenį tikslu)
- Kita

11.14. _____
_____
_____
_____
_____
_____

11.15.

2.2. Vientisumo praradimo atveju:

11.16.

- Pakeitimas į neteisingus duomenis dėl ko asmuo gali netekti galimybės naudotis paslaugomis
- Pakeitimas į galiojančius duomenis, kad asmens duomenų tvarkymas būtų nukreiptas (pavyzdžiui, pavogta asmens tapatybė susiejant vieno asmens identifikuojančius duomenis su kito asmens biometriniais duomenimis)
- Kita

_____
_____
_____
_____
_____

11.17.

2.3. Duomenų prieinamumo praradimo atveju:

- Dėl asmens duomenų trūkumo negalima teikti paslaugų (pavyzdžiui, administracinių procesų sutrikdymas, dėl ko negalima prieiti, pavyzdžiui, prie asmens sveikatos istorijų ir teikti pacientams sveikatos paslaugų, arba įgyvendinti duomenų subjekto teises)
- Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamos paslaugos (pavyzdžiui, asmens sveikatos istorijoje neliko informacijos apie asmens alergijas, tam tikra informacija iš mokesčių deklaracijos išnyko, dėl ko negalima tinkamai apskaičiuoti mokesčių ir pan.)
- Kita

_____
_____
_____
_____
_____

11.18.

2.4. Kita:

_____
_____
_____
_____
_____

11.19.

3. Priemonės, kurių imtasi, siekiant pašalinti pažeidimą ar sumažinti jo pasekmes

11.20.

3.1. Taikytos priemonės, siekiant sumažinti poveikį duomenų subjektams:

_____
_____
_____
_____
_____

3.2. Taikytos priemonės, siekiant pašalinti asmens duomenų saugumo pažeidimą:

_____
_____
_____
_____

3.3. Taikytos priemonės, siekiant, kad pažeidimas nepasikartotų:

_____
_____
_____
_____

3.4. Kita:

_____
_____
_____
_____
_____
_____

4. Siūlomos priemonės sumažinti asmens duomenų saugumo pažeidimo pasekmėms

_____
_____
_____
_____
_____

5. Duomenų subjektų informavimas apie asmens duomenų saugumo pažeidimą

5.1. Duomenys apie informavimo faktą:

11.21.

- ☐ Taip, duomenų subjektai informuoti (nurodoma data) _____
- ☐ Ne, bet jie bus informuoti (nurodoma data)_____
- ☐ Ne

11.22.

5.2. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, neinformavimo priežastys:

11.23.

- ☐ Ne, nes nekyla didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodoma kodėl)
  _____
  _____
  _____
- ☐ Ne, nes įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami (nurodomos kokios)
  _____
  _____

_____
_____

- ☐ Ne, nes įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodomos kokios)
  _____
  _____
  _____
  _____
- ☐ Ne, nes tai pareikalautų neproporcingai daug pastangų ir apie tai viešai paskelbta (arba taikyta panaši priemonė) (nurodoma kada ir kur paskelbta informacija viešai arba jei taikyta kita priemonė, nurodoma kokia ir kada taikyta)

11.24. _____
_____

- ☐ Ne, nes dar neidentifikuoti duomenų subjektai, kurių asmens duomenų saugumas pažeistas

11.25.

5.3. Informacija, kuri buvo pateikta duomenų subjektams (gali būti pridėtas pranešimo duomenų subjektui kopija):

_____
_____
_____
_____
_____

5.4. Būdas, kokiu duomenų subjektai buvo informuoti:

11.26.

- ☐ Paštu
- ☐ Elektroniniu paštu
- ☐ Kitu būdu _____

11.27.

5.5. Informuotų duomenų subjektų skaičius

_____

11.28.

6. Asmuo, galintis suteikti daugiau informacijos apie asmens duomenų saugumo pažeidimą (duomenų apsaugos pareigūnas ar kitas kontaktinis asmuo)

6.1. Vardas ir pavardė _____

11.29.

6.2. Telefono ryšio numeris

_____

11.30.

6.3. Elektroninio pašto adresas

_____

11.31.

6.4. Pareigos

11.32. _____

11.33.

6.5. Darbovietės pavadinimas ir adresas

_____

11.34.

7. Pranešimo pateikimo Valstybinei duomenų apsaugos inspekcijai pateikimo vėlavimo priežastys

_____
_____
_____
_____
_____

8. Kita reikšminga informacija

_____
_____
_____
_____
_____
_____

_____	_____	_____
(pareigos)	(parašas)	(vardas, pavardė)

_____

Asmens duomenų
tvarkymo taisyklių
6 priedas

(Asmens duomenų saugumo pažeidimų registravimo žurnalo forma)

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMO ŽURNALAS

Eil. Nr.	Pažeidimo nustatymo data, laikas ir vieta	Darbuotojas ar duomenų tvarkytojas, pranešęs apie pažeidimą (vardas, pavardė, pareigos ar pavadinimas)	Pažeidimo padarymo data ir vieta	Pažeidimo pobūdis, priežastys ir kitos aplinkybės	Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius	Asmens duomenų, kurių saugumas pažeistas, kategorijos ir apytikslis skaičius	Tikėtinos pažeidimo pasekmės bei pavojus fizinių asmenų teisėms ir laisvėms	Priemonės, kurių buvo imtasi pažeidimui pašalinti ir (ar) neigiamoms pažeidimo pasekmėms sumažinti	Informacija, ar apie pažeidimą buvo pranešta Valstybinei duomenų apsaugos inspekcijai, priimto sprendimo motyvai	Informacija, ar apie pažeidimą buvo pranešta duomenų subjektui (subjektams), priimto sprendimo motyvai	Kita informacija, susijusi su asmens duomenų saugumo pažeidimu
1.											
2.											
3.											
4.											
5.											
6.											
7.											
8.											
9.											
10.											

_____