PATVIRTINTA
Šiaulių technologijų mokymo centro
direktoriaus 2024 m. lapkričio 11 d.
įsakymu Nr. V-551

ŠIAULIŲ TECHNOLOGIJŲ MOKYMO CENTRO ASMENS DUOMENŲ TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Asmens duomenų tvarkymo taisyklių (toliau - Taisyklės) tikslas – reglamentuoti asmenų, kurių duomenis tvarko Šiaulių technologijų mokymo centras 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 - ADTAI). Bendrojo duomenų apsaugos reglamento (ES) 2016/679 (toliau BDAR), kitų teisės aktų reglamentuojančių asmens duomenų tvarkymą ir apsaugą, laikymąsi ir įgyvendinimą.

2. Centro darbuotojai, atlikdami savo pareigas ir tvarkydami asmens duomenis, privalo laikytis pagrindinių asmens duomenų tvarkymo principų bei konfidencialumo ir saugumo reikalavimų, įtvirtintų Bendrajame duomenų apsaugos reglamente, Įstatyme, kituose teisės aktuose ir šiose Taisyklėse.

3. Taisyklėse naudojamos sąvokos ir sutrumpinimai:

3.1. **ADTĮ** – Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

3.2. **asmens duomenų tvarkymas** – bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas;

3.3. **asmens duomenų saugumo pažeidimas (neatitiktis) (toliau 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;

3.4. **asmens prašymas** – bet kuris iš žemiau nurodytų:

3.4.1. prašymas susipažinti su duomenimis apie asmenį;

3.4.2. prašymas ištaisyti netikslius asmens duomenis;

3.4.3. prašymas ištrinti duomenis apie asmenį;

3.4.4. prašymas apriboti duomenų apie asmenį naudojimą ar trynimą;

3.4.5. prašymas išeksportuoti duomenis apie asmenį;

3.4.6. prieštaravimas dėl duomenų apie asmenį rinkimo, naudojimo ir saugojimo Centre;

3.4.7. prieštaravimas dėl, bet kokio automatinio sprendimo priėmimo dėl asmens ar asmens profiliavimo Centre;

3.4.8. bet kuris kitas prašymas ir (arba) skundas dėl bet kokio klausimo, susijusio su duomenų apsauga Centre.

3.5. **atsakingas darbuotojas** – darbuotojas, kuris pagal užimamas pareigas ir darbo pobūdį turi teisę vykdyti konkrečias su duomenų tvarkymu susijusias funkcijas;

3.6. **BDAR** – Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant duomenis ir dėl laisvo tokių asmenų judėjimo ir kuriuo naikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

3.7. **DAP** – duomenų apsaugos pareigūnas. Centro vadovo paskirtas darbuotojas ar paslaugų teikėjas, atliekantis BDAR nustatytas duomenų apsaugos pareigūno funkcijas;

3.8. **darbuotojas** – asmuo, kuris su Centru yra sudaręs darbo arba panašaus pobūdžio sutartį;

3.9. **duomenys apie sveikatą** – asmens duomenys, susiję su fizine ar psichine fizinio asmens sveikata, atskleidžiantys informaciją apie to fizinio asmens sveikatos būklę;

3.10. **duomenys/asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektą); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai ar netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, vardą ir pavardę, asmens indentifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius;

3.11. **duomenų bazė** – yra organizuotas (susistemintas, metodiškai sutvarkytas) duomenų rinkinys, kuriuo galima individualiai naudotis elektroniniu ar kitu būdu;

3.12. **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 tikslų atitinkančių duomenų apsaugos taisykles.

3.13. **duomenų subjektas** – fizinis asmuo, kurio asmens duomenis tvarko duomenų valdytojas arba duomenų tvarkytojas;

3.14. **duomenų tvarkymas informacinėmis ir komunikacinėmis technologijomis** - duomenų rinkimas, naudojimas, saugojimas, persiuntimas, naikinimas ar bet kuris kitas konkretus su duomenimis atliekamas veiksmas. Informacinės ir komunikacinės technologijos, kurias Centras suteikia Centre, įskaitant, bet neapsiribojant, kompiuteriais, planšetiniais kompiuteriais, išmaniaisiais telefonais, USB įrenginiais ar kitomis duomenų laikmenomis, nutolusiomis duomenų saugyklomis, interneto svetainėmis bei kita programine įranga;

3.15. **duomenų tvarkymo veiklos įrašas** – dokumentas, kuriame fiksuojama Centro vykdomų duomenų tvarkymo veiklų tikslai, duomenų subjektai, duomenų gavėjai, duomenų ištrynimo terminai ir kita reikalaujama arba reikšminga informacija apie duomenų tvarkymo veiklas;

3.16. **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 paslaugos tiekėjas ir pan.

3.17. **duomenų saugumo pažeidimo valdymas** – procesas, kurio metu Centre analizuojami, registruojami duomenų saugumo pažeidimai ir, jei reikia, teikiami pranešimai inspekcijai ar asmenims, kurių duomenys buvo paveikti;

3.18. **duomenų saugumo pažeidimas** – bet kuris iš toliau nurodytų įvykių:

3.18.1. Centro IKT, dokumentų ir (arba) kitų priemonių, kuriuose yra duomenų praradimas, vagystė arba nesuplanuotas sunaikinimas;

3.18.2. atsitiktinis ar tyčinis duomenų siuntimas, įkėlimas ar dalinimasis su trečiaisiais asmenimis, neturinčiai teisės jų gauti;

3.18.3. trečiųjų asmenų neteisėta prieiga prie Centro IKT, dokumentų ir (ar) kitų priemonių, kuriose yra duomenų;

3.18.4. kenkėjiškos atakos prieš Centro IKT ir (ar) kitas priemones, kuriose yra duomenų;

3.18.5. klaidos, susijusios su kuriamomis, naudojamomis ir konfigūruojamomis IKT ir (ar) kitomis priemonėmis, kurios gali kelti pavojų duomenų saugumui;

3.18.6. bet kokie kiti saugumo pažeidimai, lemiantys atsitiktinį ar neteisėtą duomenų sunaikinimą, praradimą, nutekėjimą, pakeitimą, neleistiną atskleidimą arba prieigos prie Centro perduodamų, saugojamų ar kitaip renkamų, naudojamų ar saugojamų duomenų suteikimą;

3.19. **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;

3.20. **duomenų valdytojas** – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones.

3.21. **duomenų tvarkytojas ir valdytojas (toliau – Centras) – Šiaulių technologijų mokymo centras, 306139052, Dvaro g. 144A, Šiauliai.**

3.22. **EEE** – Europos Ekonominė Erdvė (visos ES valstybės narės bei Islandija, Norvegija, Lichtenšteinas);

3.23. **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;

3.24. **inspekcijos paklausimas** – bet kuris laiškas, pranešimas, užklausa ar kitas dokumentas, kurį pateikia Valstybinė duomenų apsaugos inspekcija (toliau – VDAI) ir, kuris yra adresuotas Centrui;

3.25. **inspekcijos paklausimų valdymas** – procesas, kurio metu nagrinėjami inspekcijos paklausimai, renkama atsakymui reikalinga informacija ir inspekcijai pateikiamas atsakymas;

3.26. **informacinė sistema** – informacijai kurti ir perduoti skirtų priemonių visuma, sudaryta iš informacijos apdorojimo sistemos ir organizacijos išteklių (žmonių, techninių priemonių, lėšų ir pan.), reikalingų, kad ta visuma galėtų veikti;

3.27. **inventorizacija** – sistemingas procesas, kurio metu nustatomi visi organizacijos tvarkomi asmens duomenys, jų tvarkymo tikslai, teisinis pagrindas, saugojimo terminai, technines ir organizacines saugumo priemones bei kiti su asmens duomenų tvarkymu susiję reikšmingi aspektai;

3.28. **interneto svetainė** – Centro svetainė, kurioje yra pristatoma Centro veikla;

3.29. **kandidatas** – asmuo, pageidaujantis tapti Centro darbuotoju arba dalyvauti Centro vykdomoje personalo atrankoje;

3.30. **kompiuterinė įranga** – kompiuteriai, terminalai, serveriai, laikmenos, kita Centro teisėtu pagrindu (nuosavybės teise, nuomos ar kitais pagrindais) priklausanti kompiuterinė įranga ir joje esanti programinė įranga, tame tarpe elektroninė pašto dėžutė, bendravimo interneto tinklu programos, debesų kompiuterijos paslaugos, interneto prieiga;

3.31. **mokymai** – Centro organizuojami darbuotojams skirti mokymai, susiję su asmens duomenų apsaugos klausimais;

3.32. **paslaugų gavėjas** – asmuo, kuriam Centras teikia arba anksčiau teikė paslaugas;

3.33. **priežiūros institucija** – Valstybinė duomenų apsaugos inspekcija (toliau - VDAI);

3.34. **specialių kategorijų asmens duomenys** – asmens duomenys, atskleidžiantys fizinio asmens rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, genetiniai duomenys, biometriniai duomenys, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenys, duomenys apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją;

3.35. **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;

3.36. **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 tvarkytojo įgaliojimu leidžiama tvarkyti asmens duomenis. Pavyzdžiui: partneriai, tiekėjai, nuomotojai, Valstybinė mokesčių inspekcija, bankai ir pan.;

3.37. **vaizdo stebėjimas** – vaizdo duomenų, susijusių su fiziniu asmeniu tvarkymas Centre;

4. Kitos, aukščiau nenurodytos Taisyklėse vartojamos sąvokos atitinka ADTAĮ ir BDAR vartojamas sąvokas.

5. Taisyklės taikomos tvarkant fizinių asmenų duomenis tiek autonominiu būdu, tiek neautonominiu būdu tvarkant asmens duomenų susistemintas rinkmenas, mokinių bylas ir kt..

6. Taisyklės privalomos visiems Centre pagal darbo sutartis dirbantiems darbuotojams (toliau – darbuotojas), kurie įgalioti tvarkyti Centre esančius asmens duomenis arba eidami savo pareigas juos sužino, bei kitiems sutartiniais pagrindais paslaugas teikiantiems asmenims, kurie gali tvarkyti arba sužino asmens duomenis.

II SKYRIUS
ASMENS DUOMENŲ TVARKYMO TIKSLAI IR PRINCIPAI

7. Centras asmens duomenis tvarko šiais tikslais:

7.1. vidaus administravimo (pvz.: mokinio priėmimo į mokyklą organizavimas ir administravimas; mokinio maitinimo organizavimo ir stipendijų mokėjimo; akademinių atostogų suteikimo; sąskaitos išdavimo tikslu; turto perdavimo organizavimo; darbo užmokesčio priskaitymo ir išmokėjimo; darbuotojų priėmimo planavimo ir darbo organizavimo; darbuotojo darbo laiko apskaitos organizavimo; darbuotojų veiklos vertinimo; sutarčių (įsipareigojimo) sudarymo, įgyvendinimo; sveikatos tikrinimo; turto valdymo priežiūros; paslaugų planavimo, organizavimo ir vykdymo (pvz.: apgyvendinimo, maitinimo, bibliotekos, Autodromo, Kartodromo, Autoserviso, Fizinės ir medicininės reabilitacijos centro „Gelmės“ paslaugų) ir kt.);

7.2. mokymo proceso organizavimo (pvz.: mokymo sutarčių sudarymo/nutraukimo, mokinių atsiskaitymas, tvarkaraščio sudarymas, dienynų pildymas, nuotolinės mokymosi sistemos administravimo ir kt.) tikslais;

7.3. nuosavybės teise ar kitu teisiniu pagrindu Centro valdomų materialinių išteklių (toliau – turtas) apsaugą, asmenų apsaugos bei vairavimo mokymo tobulinimo tikslu (pvz.: vaizdo stebėjimo ir tvarkymo, pašalinių asmenų patekimo į Centrą ar į bendrabutį ir kt.);

7.4. projektų finansuojamų Europos Sąjungos lėšomis (pvz.: projektų dalyvių registravimo ir administravimo; ataskaitų rengimo ir pateikimo; projektų auditų ir patikrų vykdymo; mokėjimų valdymo; komunikacijos ir viešinimo; projektų dokumentacijos tvarkymo ir archyvavimo; projekto tikslų ir rezultatų stebėjimo ir vertinimo; ir kt.) , Centro renginių, konkursų įgyvendinimo tikslu;

7.5. rinkodaros ir komunikacijos (renginių viešinimo; paslaugų viešinimo; naujienlaiškių siuntimo; renginių, konkursų ir akcijų organizavimo; socialinių tinklų administravimo; rinkos tyrimų ir apklausų; klientų segmentavimo; komunikacijos efektyvumo vertinimo ir kt.);

7.6. kitiems duomenų tvarkymo tikslams, kurie nėra tiesiogiai nurodyti šiose Taisyklėse, bet yra patvirtinti direktoriaus arba yra reglamentuoti kituose Centre galiojančiuose tvarkos aprašuose ar taisyklėse. Tokiais atvejais duomenų tvarkymo pagrįstumas turi būti įvertintas ir patvirtintas duomenų apsaugos pareigūno arba Centro direktoriaus.

8. Centro duomenų tvarkymo tikslų sritys aiškiai apibrėžtos duomenų valdytojo/tvarkytojo duomenų tvarkymo veiklos įrašuose pagal konkrečius tvarkomus dokumentus.

9. Centre gali būti tvarkomi ir kitų kategorijų asmens duomenys kitais tikslais, jeigu toks asmens duomenų tvarkymas yra grindžiamas Bendrajame duomenų apsaugos reglamente nurodytais pagrindais.

10. Taisyklių 7.1. – 7.6. punktuose nurodytus ir kitus Centro tvarkomus asmens duomenis tvarko Centro darbuotojai, kuriems tokius asmens duomenis tvarkyti būtina jų darbo funkcijų atlikimui.

11. Asmens duomenys Centre gali būti tvarkomi tik esant bent vienam iš šių pagrindų:

11.1. sutartis: duomenys reikalingi siekiant sudaryti ar vykdyti darbo, civilinę ar kitokią sutartį su Asmeniu, įskaitant, bet neapsiribojant sutarties sąlygų vykdymą, teisės aktų atitinkamai sutarties rūšiai numatytų šalių teisių ir pareigų vykdymą ir iš sutarties esmės kylančių šalių įsipareigojimų vykdymą;

11.2. teisinė prievolė: Centras teisės aktais yra įpareigotas tvarkyti Duomenis mokesčių, darbo, socialinės apsaugos ir kitose srityse;

11.3. užduočių, vykdomų viešojo intereso labui, arba pavestų viešosios valdžios funkcijų vykdymas: duomenys yra reikalingi socialinių paslaugų, teikiamų valstybės ir/ar vietos savivaldos

pavedimu, teikimui ir/ar administravimui, jei Asmens interesai konkrečių aplinkybių kontekste nėra svarbesni.

11.4. sutikimas (Taisyklių 2 priedas): Asmuo galėjo laisvai pasirinkti, ar duoti sutikimą dėl jo Duomenų tvarkymo, be jokių neigiamų pasekmių Asmeniui ir tokį sutikimą davė. Sutikimą asmuo pildo personalo skyriuje.

12. Centras specialiųjų kategorijų asmens duomenis tvarko tik esant bent vienam iš šių pagrindų:

12.1. tvarkyti duomenis būtina, kad duomenų valdytojas arba duomenų subjektas galėtų vykdyti 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 subjektų pagrindinių teisių ir interesų apsaugos priemonės;

12.2. tvarkyti duomenis būtina, kad būtų apsaugoti gyvybiniai duomenų subjektų arba kito fizinio asmens interesai, kai duomenų subjektas dėl fizinių ar teisinių priežasčių negali duoti sutikimo;

12.3. tvarkomi asmens duomenys, kuriuos duomenų subjektas yra akivaizdžiai paskelbęs viešai;

12.4. tvarkyti duomenis būtina siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus;

12.5. 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;

12.6. tvarkyti duomenis būtina profilaktinės arba darbo medicinos tikslais, siekiant įvertinti darbuotojo darbingumą;

12.7. tvarkyti duomenis būtina siekiant valdyti sveikatos priežiūros sistemas ir paslaugas remiantis Europos Sąjungos arba valstybės narės teise;

12.8. tvarkyti duomenis būtina dėl viešojo intereso priežasčių visuomenės sveikatos srityje, pavyzdžiui, siekiant apsisaugoti nuo rimtų tarpvalstybinio pobūdžio grėsmių sveikatai arba užtikrinti aukštus sveikatos priežiūros ir vaistų arba medicinos priemonių kokybės ir saugos standartus, remiantis Sąjungos arba valstybės narės teise.

13. Centras užtikrina BDAR 5 str. nustatytus su asmens duomenų tvarkymu susijusius principus:

13.1. **teisėtumo, sąžiningumo ir skaidrumo principas –** asmens duomenys turi būti duomenų subjekto atžvilgiu tvarkomi teisėtu, sąžiningu ir skaidriu būdu;

13.2. **tikslo apribojimo principas** – asmens duomenys turi būti renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu. Tolesnis duomenų tvarkymas archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais nėra laikomas nesuderinamu su pirminiais tikslais. Centro darbuotojai turi teisę rinkti, tvarkyti, perduoti, saugoti, naikinti ar kitaip naudoti asmens duomenis tik atlikdami savo tiesiogines funkcijas, apibrėžtas pareigybės aprašyme ar kitame Centro lokaliniame teisės akte arba Centro vadovo pavedimu ir tik teisės aktų nustatyta tvarka. Centro darbuotojams draudžiama savarankiškai rinkti, tvarkyti, perduoti, saugoti, naikinti ar kitaip naudoti asmens duomenis;

13.3. **duomenų kiekio mažinimo principas** – asmens duomenys turi būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi;

13.4. **tikslumo principas** – 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;

13.5. **saugojimo trukmės apribojimo principas** – asmens duomenys turi būti laikomi 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, reikalingų siekiant apsaugoti duomenų subjekto teises ir laisves;

13.6. **vientisumo ir konfidencialumo principas** – asmens duomenys turi būti 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;

13.7. **atskaitomybės principas** – Duomenų valdytojas yra atsakingas ir turi sugebėti įrodyti, kad laikomasi aukščiau nurodytų principų.

14. Asmens duomenų tvarkymo principų laikymąsi užtikrina Centro vadovas ir jo įgalioti darbuotojai, imdamiesi atitinkamų organizacinių priemonių (įsakymai, nurodymai, rekomendacijos, pavedimai ir pan.), kad būtų įgyvendintos Duomenų valdytojui priskirtos prievolė. (Pavyzdžiui: įpareigoti nutraukti neteisėtus ar asmens duomenų apsaugos reikalavimus pažeidžiančius duomenų tvarkymo veiksmus, sunaikinti dokumentų, kuriuose yra nurodyti asmens duomenys, kopijas ir pan.).

15. Duomenys tvarkomi tinkamai informavus Duomenų subjektus laikantis BDAR nustatytų reikalavimų.

16. Duomenys saugomi laikotarpius, nurodytus Centro dokumentacijos plane.

17. Pasibaigus duomenų saugojimo terminui asmens duomenys yra visam laikui ištrinami, sunaikinami, išskyrus, jei teisės aktai numato kitaip.

18. Sunaikinimas apibrėžiamas kaip fizinis ar techninis veiksmas, kuriuo duomenys padaromi neatkuriami:

18.1. elektronine forma saugomi asmens duomenys sunaikinami juos ištrinant be galimybės atkurti;

18.2. popieriniai dokumentai, kuriuose yra asmens duomenų, susmulkinami, o likučiai saugiu būdu sunaikinami.

19. Jeigu duomenys naudojami kaip įrodymai civilinėje, administracinėje ar baudžiamojoje byloje ar kitais įstatymų nustatytais atvejais, duomenys gali būti saugomi tiek, kiek reikalinga šiems duomenų tvarkymo tikslams, ir sunaikinami nedelsiant, kai tampa nebereikalingi.

20. Centro, kaip duomenų valdytojo tvarkomi duomenys yra saugomi atsakingiems darbuotojams priskirtuose dokumentuose, kompiuteriuose, programų sistemose. Prieiga prie Duomenų suteikiama tik Atsakingiems darbuotojams ir asmenims turintiems teisę prieiti prie duomenų.

21. Asmens duomenų perdavimas Centro viduje vyksta darbuotojams susirašinėjant darbo el. paštu, perduodant rašytinius dokumentus, naudojantis kitomis informacinėmis sistemomis.

22. Centro tvarkomus asmens duomenis, Centras gali perduoti tretiesiems asmenims vykdant teisės aktuose įtvirtintas Centro pareigas, valstybės ir (ar) savivaldos institucijų nurodymus bei kitų teisės aktų nustatytais atvejais ir tvarka.

23. Duomenų tvarkytojo prieigos teisės prie duomenų naikinamos nutraukus asmens duomenų tvarkymo sutartį sudarytą su Centru, ar šiai sutarčiai nustojus galioti.

24. Atsakingi darbuotojai privalo:

24.1. tvarkyti asmens duomenis vadovaudamiesi Europos Sąjungos ir Lietuvos Respublikos teisės aktais, taip pat šiomis Taisyklėmis ir jos priedais;

24.2. neatskleisti, neperduoti ir nesudaryti sąlygų, bet kokiomis priemonėmis susipažinti su duomenimis asmenims, kurie nėra įgalioti tvarkyti duomenų;

24.3. nedelsiant pranešti Centro direktoriui apie bet kokią įtartiną situaciją, kuri gali kelti grėsmę duomenų saugumui.

25. Atsakingas darbuotojas netenka teisės tvarkyti asmens duomenis, kai pasibaigia atsakingo darbuotojo darbo sutartis su Centru arba, kai pasikeitus darbuotojo užimamoms pareigoms asmens duomenys tampa nebereikalingi darbo funkcijoms vykdyti.

26. Duomenys perduodami duomenų tvarkytojams ir duomenų gavėjams kai teisę ir (ar) pareigą tai daryti atitinkamais pagrindais suteikia teisės aktai.

27. Asmens duomenys Centre gali būti pateikti ikiteisminio tyrimo įstaigai, prokurorui ar teismui dėl administracinių, civilinių, baudžiamųjų bylų, kaip įrodymai ar kitais teisės aktų nustatytais atvejais. Centras gali pateikti asmens duomenis savo duomenų tvarkytojams, kurie teikia Centrui paslaugas ir tvarko asmens duomenis Centro vardu. Duomenų tvarkytojai turi teisę tvarkyti asmens duomenis tik pagal Centro nurodymus ir tik ta apimtimi, kiek tai yra būtina siekiant tinkamai vykdyti sutartyje nustatytus įsipareigojimus. Centras pasitelkia tik tuos duomenų tvarkytojus, kurie pakankamai užtikrina, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokius būdu, kad duomenų tvarkymas atitiktų BDAR reikalavimus ir būtų užtikrinta duomenų subjektų teisių apsauga.

28. Centro darbuotojai, kurie tvarko asmens duomenis arba kuriems suteikta prieiga prie asmens duomenų, privalo laikytis konfidencialumo principo ir laikyti paslaptyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jie susipažįsta vykdydami savo pareigas (Taisyklių 1 priedas). Konfidencialumo įsipareigojimą esami ir būsimi Centro darbuotojai pasirašo personalo skyriuje. Pareiga saugoti asmens duomenų paslaptį galioja visiems Centro darbuotojams, taip pat ir perėjus dirbti į kitas pareigas, pasibaigus darbo ar sutartiniams santykiams.

III SKYRIUS
DUOMENŲ VALDYTOJO IR TVARKYTOJO FUNKCIJOS, TEISĖS IR PAREIGOS

29. Centras, veikdamas kaip duomenų valdytojas, yra atsakingas už duomenų tvarkymo tikslų ir priemonių nustatymą bei užtikrinimą, kad duomenų tvarkymas vyktų teisėtai ir atitiktų BDAR reikalavimus.

30. Duomenų valdytojas organizuoja duomenų tvarkymą taip, kad būtų užtikrintas asmens duomenų apsaugos principų laikymasis:

30.1. teisėtumo, sąžiningumo ir skaidrumo – duomenys turi būti tvarkomi teisėtai ir skaidriai.

30.2. tikslo apribojimo – duomenys renkami nustatytais ir aiškiai apibrėžtais tikslais.

30.3. duomenų kiekio mažinimo – duomenys turi būti adekvatūs ir tik tie, kurie būtini tikslui pasiekti.

30.4. tikslumo – duomenys turi būti tikslūs ir, jei reikia, atnaujinami.

30.5. saugojimo trukmės apribojimo – duomenys turi būti laikomi ne ilgiau, nei būtina.

30.6. vientisumo ir konfidencialumo – duomenys turi būti apsaugoti nuo neteisėtos prieigos ar praradimo.

30.7. atskaitomybės – Centras atsako už principų laikymąsi ir turi tai įrodyti.

31. Duomenų valdytojo teisės:

31.1. priimti ir keisti vidaus tvarkos dokumentus, susijusius su duomenų tvarkymu.

31.2. skirti atsakingus asmenis, įgaliotus vykdyti duomenų tvarkymo funkcijas.

31.3. sudaryti duomenų tvarkymo sutartis su duomenų tvarkytojais.

31.4. prižiūrėti asmens duomenų tvarkymo procesus, užtikrinant jų atitiktį teisės aktų reikalavimams.

32. Duomenų valdytojo pareigos:

32.1. užtikrinti, kad duomenų subjektų teisės būtų įgyvendintos pagal BDAR ir Lietuvos teisės aktus.

32.2. įgyvendinti tinkamas organizacines ir technines saugumo priemones, apsaugančias duomenis nuo neteisėtos prieigos, praradimo ar pažeidimo.

32.3. pasirinkti tik tuos duomenų tvarkytojus, kurie garantuoja, kad laikomasi BDAR reikalavimų.

32.4. atlikti poveikio duomenų apsaugai vertinimą, jei duomenų tvarkymas gali kelti aukštą riziką asmenų teisėms ir laisvėms.

33. Duomenų tvarkytojo funkcijos:

33.1. duomenų tvarkytojas vykdo duomenų tvarkymą Centro nurodymu ir tik pagal Centro nustatytus duomenų tvarkymo tikslus ir priemones.

33.2. padeda Centrui užtikrinti BDAR reikalavimus, įgyvendindamas duomenų apsaugos priemones.

34. Duomenų tvarkytojo teisės:

34.1. tvarkyti duomenis tik tose apimtyse ir tikslais, kuriuos numatė Centras.

34.2. teikti siūlymus dėl duomenų tvarkymo procesų ir techninių priemonių tobulinimo, siekiant efektyvesnės apsaugos.

35. Duomenų tvarkytojo pareigos:

35.1. įgyvendinti technines ir organizacines priemones, užtikrinančias, kad asmens duomenys būtų apsaugoti nuo neteisėto tvarkymo ar praradimo.

35.2. uždrausti asmens duomenis naudoti bet kokiems nenumatytiems tikslams, nebent tam būtų gautas Centro leidimas.

35.3. užtikrinti, kad darbuotojai, kuriems suteikta prieiga prie asmens duomenų, laikytųsi konfidencialumo principo.

36. Atsakomybė ir pranešimų tvarka:

36.1. Duomenų valdytojas atsako už duomenų tvarkymo teisėtumą, ir prireikus praneša VDAI apie asmens duomenų saugumo pažeidimus.

36.2. Pažeidimo atveju duomenų valdytojas turi imtis skubių veiksmų, kad išspręstų problemą ir sumažintų galimą žalą.

IV SKYRIUS
DUOMENŲ TVARKYTOJŲ PASITELKIMAS ASMENS DUOMENŲ TVARKYMUI

37. Kai asmens duomenys Centro vardu tvarkomi pasitelkiant duomenų tvarkytojus, darbuotojai, kurie vykdydami savo funkcijas Centro vardu ketina pasitelkti duomenų tvarkytojus, privalo apie tai iš anksto pranešti duomenų apsaugos pareigūnui. Tokiu atveju, duomenų apsaugos pareigūnas privalo užtikrinti, jog būtų pasitelkiami tik tie duomenų tvarkytojai, kurie pakankamai užtikrina, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad asmens duomenys būtų tvarkomi laikantis Bendrojo duomenų apsaugos reglamento, Įstatymo ir kitų teisės aktų reikalavimų, bei kad būtų užtikrinta asmens duomenų subjektų teisių apsauga.

38. Tuo atveju, jeigu asmens duomenų tvarkymui Centras pasitelkia duomenų tvarkytojus, duomenų apsaugos pareigūnas privalo užtikrinti (parengti/suderinti sutarties projektą), jog Centras su tokiais duomenų tvarkytojais būtų pasirašęs sutartis, kurioje būtų nustatomi duomenų tvarkymo dalykas ir trukmė, duomenų tvarkymo pobūdis ir tikslas, asmens duomenų rūšis ir duomenų subjektų kategorijos bei Centro prievolės ir teisės. Atitinkamoje sutartyje duomenų tvarkytojui turi būti nustatytos visos pareigos ir sąlygos, nurodytos Bendrojo duomenų apsaugos reglamento 28 str. 3 dalyje.

V SKYRIUS
DUOMENŲ TEIKIMAS TRETIESIEMS ASMENIMS

39. Centras teikia asmens duomenis duomenų gavėjams – tretiesiems asmenims ir duomenų tvarkytojams.

40. Asmens duomenys teikiami tretiesiems asmenims:

40.1. valstybės institucijoms ir įstaigoms;

40.2. teismams;

40.3. teisėsaugos institucijoms;

40.4. kitiems tretiesiems asmenims, kuriems teikti asmens duomenis Centrą įpareigoja įstatymai ar kiti teisės aktai, arba tada, kai asmens duomenis teikti būtina vykdant Centro pavestas funkcijas, įgyvendinant Centro, kaip darbdavio pareigas, vadovaujantis Reglamentu arba vykdant sutartis.

41. Asmens duomenys tretiesiems asmenims teikiami pagal asmens duomenų teikimo sutartį (daugkartinis asmens duomenų teikimas), pagal pirkimo sutartis (pirkimo sutarčių vykdymas), pagal prašymą (vienkartinis asmens duomenų teikimas) arba teisės aktų nustatyta tvarka.

42. Jeigu asmens duomenys teikiami pagal asmens duomenų teikimo sutartį arba pagal pirkimo sutartį, kai duomenų gavėjas yra asmens duomenų valdytojas, joje turi būti nurodytas asmens duomenų naudojimo tikslas, teikimo ir gavimo teisinis pagrindas, sąlygos, jame turi būti nurodytas asmens duomenų naudojimo tikslas, teikimo ir gavimo teisinis pagrindas, prašomų pateikti asmens duomenų apimtis.

43. Asmens duomenys tretiesiems asmenims teikiami tik esant asmens duomenų teikimo teisiniam pagrindui, įvertinus asmens duomenų tvarkymo tikslą ir teikiamų asmens duomenų apimtį.

44. Centras gali teikti asmens duomenis duomenų tvarkytojams, kurie teikia paslaugas Centrui ar atlieka kitus darbus ir tvarko asmens duomenis Centro, kaip duomenų valdytojo, vardu.

45. Centro pasitelkiami duomenų tvarkytojai turi užtikrinti, kad asmens duomenų tvarkymo techninės ir organizacinės priemonės bus įgyvendinamos taip, kad duomenų tvarkymas atitiktų Reglamento reikalavimus ir būtų užtikrinta duomenų subjekto teisių apsauga.

46. Nuostatos, susijusios su asmens duomenų tvarkymu ir apsauga, įtraukiamos į su duomenų tvarkytojais sudaromas sutartis, kuriose turi būti nurodytos šios sąlygos:

46.1. asmens duomenų tvarkymo dalykas ir trukmė;

46.2. asmens duomenų tvarkymo tikslas ir pobūdis;

46.3. asmens duomenų rūšis ir duomenų subjektų kategorijos;

46.4. duomenų valdytojo ir duomenų tvarkytojo teisės ir prievolės;

46.5. leidimas arba ne duomenų tvarkytojui pasitelkti kitą duomenų tvarkytoją;

46.6. duomenų tvarkytojo įsipareigojimas vykdant sutartį gauti asmens duomenis tvarkyti Centro vardu ir tik pagal Centro nurodymus laikantis duomenų apsaugą reglamentuojančių teisės aktų reikalavimų;

46.7. duomenų tvarkytojo įsipareigojimas įgyvendinti tinkamas technines, organizacines ir teisines asmens duomenų apsaugos priemones, kad būtų užtikrintas perduodamų asmens duomenų saugumas;

46.8. duomenų tvarkytojo įsipareigojimas padėti Centrui įgyvendinti duomenų subjekto teises;

46.9. duomenų tvarkytojo įsipareigojimas pateikti Centrui visą informaciją, būtiną siekiant įsitikinti ir įrodyti, kad asmens duomenys tvarkomi teisėtai, ir sudaryti sąlygas bei padėti Centrui arba Centro įgaliotam asmeniui atlikti asmens duomenų tvarkymo auditą, įskaitant patikrinimus;

46.10. duomenų tvarkytojo įpareigojimas, atsižvelgiant į duomenų tvarkymo pobūdį ir duomenų tvarkymo turimą informaciją, padėti Centrui įgyvendinti teisės aktuose įtvirtintas pareigas, susijusias su įvykusiu asmens duomenų saugumo pažeidimu, poveikio duomenų apsaugai vertinimu ir išankstinėmis konsultacijomis;

46.11. draudimas duomenų tvarkytojui perduotus asmens duomenis naudoti asmens duomenų tvarkymo sutartyse nenurodytais tikslais ar savo rinkodaros tikslais;

46.12. duomenų tvarkytojo įsipareigojimas atsakyti už neteisėtą asmens duomenų tvarkymą ir atlyginti Centrui dėl duomenų tvarkytojo vykdyto neteisėto asmens duomenų tvarkymo patirtus nuostolius, sumokėtas baudas ar kompensacijas;

46.13. duomenų tvarkytojo įsipareigojimas pasibaigus sutarčiai sunaikinti perduotus asmens duomenis arba grąžinti juos Centrui;

46.14. kitos sąlygos, būtinos siekiant užtikrinti perduotų asmens duomenų tvarkymo teisėtumą ir saugumą.

47. Į neįgaliotų trečiųjų asmenų elektroninius ar kitokia forma (išskyrus telefonu) pateiktus prašymus suteikti jiems informaciją apie duomenų subjektus turi būti atsakoma tik jeigu rašytiniame prašyme yra nurodytas duomenų subjekto duomenų naudojimo tikslas, tinkamas teikimo bei gavimo teisinis pagrindas ir prašomų pateikti duomenų subjektų duomenų apimtis.

Informacija (asmens duomenys) apie paslaugų gavėją telefonu neatskleidžiama jei neįmanoma identifikuoti paslaugų gavėjo.

48. Vienkartinio duomenų teikimo atveju, Centras, teikdamas asmens duomenis pagal duomenų gavėjo rašytinį prašymą, prioritetą teikia duomenų teikimui elektroninių ryšių priemonėmis.

49. Konfidencialumo reikalavimas netaikomas ir informacija (asmens duomenys) gali būti suteikta tik:

49.1. tarnybiniais tikslais, neturint raštiško paslaugų gavėjo sutikimo;

49.2. institucijoms, kontroliuojančioms Centro veiklą;

49.3. teismui, prokuratūrai, ikiteisminio tyrimo įstaigoms, savivaldybių skyriams bei kitoms institucijoms, kurioms tokią teisę suteikia Lietuvos Respublikos įstatymai.

VI SKYRIUS
TECHNINĖS IR ORGANIZACINĖS ASMENS DUOMENŲ SAUGUMO PRIEMONĖS

50. Centras, atsižvelgdamas į asmens duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat į jų neteisėto tvarkymo tikimybę ir galimas to pasekmes fizinių asmenų teisėms ir laisvėms, įgyvendina technines ir organizacines priemones, kad užtikrintų ir galėtų įrodyti, jog asmens duomenys Centre tvarkomi laikantis Reglamento, asmens duomenų teisinės apsaugos įstatymo, kitų teisės aktų, reglamentuojančių asmens duomenų ir privatumo apsaugą, reikalavimų.

51. Centras atsižvelgdamas į darbuotojo einamas pareigas, savo nuožiūra darbuotojams suteikia darbo priemones. Centrui 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 Centras su darbuotoju nesutaria kitaip.

52. Atsarginės asmens duomenų kopijos daromos, atsižvelgiant į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį ir tikslus, taip pat atsižvelgiant į duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms.

53. Centre įgyvendinamos organizacinės ir techninės duomenų saugumo priemonės užtikrina tokį saugumo lygį, kuris atitinka Centro valdomų duomenų pobūdį ir jų tvarkymo keliamą riziką. Rizika vertinama vadovaujantis Valstybinės duomenų apsaugos inspekcijos 2024 m. rugpjūčio 13 d. „Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairėmis duomenų valdytojams ir duomenų tvarkytojams“ (4 versija).

54. Centro organizacinės ir techninės duomenų saugumo priemonės turi užtikrinti pirmąjį automatiniu būdu tvarkomų asmens duomenų saugumo lygį. Siekiant apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, nuo bet kokio kito neteisėto tvarkymo turi būti taikomos tokios infrastruktūrinės, administracinės ir telekomunikacinės (elektroninės) priemonės:

54.1. tinkamas techninės įrangos išdėstymas ir priežiūra, informacinių sistemų priežiūra, tinklo valdymas, naudojimosi internetu saugumo užtikrinimas ir kitos informacinių technologijų priemonės. Už šių priemonių įgyvendinimą ir priežiūrą atsako Centro direktoriaus įsakymu paskirtas asmuo arba dirbantis asmuo pagal pareigybės aprašymą;

54.2. griežtas priešgaisrinės apsaugos tarnybos nustatytų normų laikymasis. Už šios priemonės įgyvendinimą atsako Centro direktoriaus įsakymu paskirtas asmuo arba dirbantis asmuo pagal pareigybės aprašymą;

54.3. tinkamas darbo organizavimas ir kitos administracinės priemonės. Už šių priemonių įgyvendinimą atsako Centro direktoriaus įsakymu paskirtas asmuo arba dirbantis asmuo pagal pareigybės aprašymą;

54.4. Centro direktoriaus įsakymu paskirtas IT specialistas ar išorės tiekėjas atsako, kad Centro Informacinių sistemų duomenų tvarkymo keliamos rizikos vertinimas būtų atliekamas periodiškai;

54.5. atsižvelgus į rizikos vertinimo rezultatus, diegiant reikiamas duomenų saugumo priemones;

54.6. patikrinant avarinio asmens duomenų atkūrimo tvarką atliekant praktinius bandymus.

55. Centro direktoriaus įsakymu paskirtas IT specialistas ar išorės tiekėjas atsako, kad duomenų atsarginių kopijų darymas ir atkūrimas būtų atliekamas:

55.1. praradus duomenis dėl aparatinės kompiuterių įrangos gedimo, programinės įrangos klaidos ir kitaip pažeidus duomenų vientisumą, duomenis atkuriant iš paskutinių turimų atsarginių duomenų kopijų;

55.2. atlikus duomenų atkūrimą, atliekant informacinės sistemos funkcionalumo ir duomenų vientisumo bei parengtumo testavimą;

55.3. periodiškai, bet ne rečiau kaip vieną kartą metuose, vykdant bandomąjį duomenų atkūrimą, užtikrinant, kad informacinių sistemų testavimas nebūtų vykdomas su realiais asmens duomenimis.

56. Darbuotojai, kurie tvarko duomenų subjektų duomenis, turi laikytis konfidencialumo principo ir laikyti paslaptyje, bet kokią su duomenų subjekto duomenimis susijusią informaciją, su kuria jie susipažino vykdydami savo pareigas. Ši pareiga išlieka galioti perėjus dirbti į kitas pareigas Centre arba pasibaigus darbo sutartiniams santykiams su Centru.

57. Darbuotojai automatiniu būdu tvarkyti asmens duomenis gali tik po to, kai jiems suteikiama prieigos teisė prie atitinkamos informacinės sistemos. Prieiga prie asmens duomenų gali būti suteikta tik tam asmeniui, kuriam asmens duomenys yra reikalingi jo darbo funkcijoms vykdyti. Darbo santykiams pasibaigus, darbuotojui prieigos prie registrų ir kitų programų teisės panaikinamos.

58. Darbuotojai gali perduoti dokumentus, kuriuose nurodyti asmens duomenys, tik tiems darbuotojams, kurie pagal pareigas ar atskirus pavedimus turi teisę dirbti su asmens duomenimis.

59. Darbuotojai, vykdantys duomenų subjekto duomenų tvarkymo funkcijas, turi užkirsti kelią atsitiktiniam ar neteisėtam tvarkymui, turi saugoti dokumentus tinkamai ir saugiai (vengiant nereikalingų kopijų su duomenų subjekto duomenimis kaupimo ir kt.). Dokumentų kopijos, kuriose nurodomi duomenų subjekto duomenys, turi būti sunaikinamos tokiu būdu, kad šių dokumentų nebūtų galima atkurti ir atpažinti jų turinio.

60. Darbuotojai, kurių kompiuteriuose saugomi duomenų subjektų duomenys arba iš kurių kompiuterių galima patekti į Centro informacines sistemas, kuriose yra saugomi duomenų subjektų duomenys, savo kompiuteriuose turi naudoti slaptažodžius „svečio“ („guest“) tipo, t. y. neapsaugoti slaptažodžiais, vartotojai yra draudžiami. Šiuose kompiuteriuose taip pat reikia naudoti ekrano užsklandą su slaptažodžiu. Prieigos prie asmens duomenų slaptažodžiai:

60.1. suteikiami, keičiami ir saugomi užtikrinant jų konfidencialumą;

60.2. unikalūs, sudaryti iš ne mažiau kaip 8 simbolių, nenaudojant asmeninio pobūdžio informacijos;

60.3. keičiami ne rečiau kaip kartą per 2 mėnesius, o esant būtinybei (pasikeitus darbuotojui, iškilus įsilaužimo grėsmei ir pan.) – nedelsiant.

61. Darbuotojų kompiuteriai, kuriuose saugomos rinkmenos su duomenų subjektų duomenimis negali būti laisvai prieinami iš kitų tinklo kompiuterių. Šių kompiuterių antivirusinė programinė įranga turi būti nuolatos atnaujinama.

62. Nesant būtinybės rinkmenos su duomenų subjekto duomenimis neturi būti dauginamos skaitmeniniu būdu, t. y. kuriamos rinkmenų kopijos vietiniuose kompiuterių diskuose, nešiojamose laikmenose, nuotolinėse rinkmenų talpyklose ir kt.

63. Centre yra užtikrinamas saugių protokolų ir (arba) slaptažodžių naudojimas, kai asmens duomenys perduodami išoriniais duomenų perdavimo tinklais.

64. Asmens duomenų, esančių išorinėse duomenų laikmenose ir elektroniniame pašte, saugos kontrolė ir ištrynimas po jų panaudojimo užtikrinamas perkeliant juos į duomenų bazes.

65. Darbuotojai privalo taip organizuoti savo darbą, kad kiek įmanoma apribotų galimybę kitiems asmenims (kitiems Centro darbuotojams, praktikantams ar kitiems asmenims) sužinoti tvarkomus Asmens duomenis. Ši nuostata įgyvendinama:

65.1. 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 asmens duomenimis;

65.2. dokumentus laikant taip, kad jų (ar jų fragmentų) negalėtų perskaityti atsitiktiniai asmenys;

65.3. jei dokumentai, kuriose yra asmens duomenų, kitiems darbuotojams, padaliniams, 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 duomenų subjektams asmeniškai ar konfidencialiai.

66. Darbuotojams, naudojantiems elektroninį paštą, interneto prieigą ir kitą informacinių technologijų ir telekomunikacijų įrangą, draudžiama:

66.1. siųsti elektroninio pašto žinutes, naudojantis kito asmens arba neegzistuojančiu elektroniniu pašto adresu;

66.2. siųsti elektroninio pašto žinutes, nuslepiant savo tapatybę;

66.3. negavus Centro vadovo sutikimo, siųsti elektroninius laiškus, kuriuose yra informacija pripažįstama konfidencialia informacija ar Centro komercine paslaptimi, išskyrus, jei informacija siunčiama asmeniui, kuris turi teisę gauti šią informaciją;

66.4. negavus Centro vadovo sutikimo perduoti, platinti, atskleisti tretiesiems asmenims darbui su technine ir programine įranga jiems suteiktus prieigos vardus, slaptažodžius ar kitus duomenis;

66.5. kurti ir platinti laiškus, skatinančius gavėją siųsti laiškus kitiems. Laiškai su perspėjimais dėl kompiuterių virusų, telefonų pasiklausymų ar kitų tariamų reiškinių, kuriuose prašoma nusiųsti gautą laišką visiems kolegoms, draugams ar pažįstamiems, turi būti nedelsiant ištrinami. Jei pranešimas sukelia įtarimų, prieš jį pašalinant, pranešti IT specialistui arba tiesioginiam vadovui;

66.6. naudoti interneto prieigą ir elektroninį paštą asmeniniams tikslams, Lietuvos Respublikos įstatymais draudžiamai veiklai, šmeižiančio, įžeidžiančio, grasinančio pobūdžio ar visuomenės dorovės ir moralės principams prieštaraujančiai informacijai, kompiuterių virusams, masinei nepageidaujamai informacijai „spam“ siųsti ar kitiems tikslams, galintiems pažeisti Centro ar kitų asmenų teisėtus interesus;

66.7. atlikti veiksmus, pažeidžiančius fizinio ir 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;

66.8. 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;

66.9. apeiti ar kitaip pažeisti bet kurio kompiuterio, tinklo ar paskyros autentifikacijos arba saugumo sistemas;

66.10. ardyti ar išmontuoti ar kitaip keisti kompiuterinę įrangą;

66.11. perkopijuoti programinę įrangą;

66.12. savarankiškai keisti kompiuterių ar kitų prietaisų tinklo parametrus (IP adresą ir pan.), savarankiškai keisti, taisyti informacinių technologijų ir telekomunikacijų techninę ir programinę įrangą;

66.13. savavališkai keisti interneto naršyklės ir elektroninio pašto programinės įrangos parametrus, susijusius su apsauga arba prisijungimo būdu, nepaisyti bet kurio iš saugumo mechanizmų;

66.14. atlikti bet kokius kitus su darbo funkcijų vykdymu nesusijusius ir teisės aktams prieštaraujančius veiksmus;

66.15. neįgaliotiems asmenims Centre ar už Centro ribų naudoti ir perduoti slaptažodžius ir kitus duomenis, kuriais pasinaudojus programinėmis ir techninėmis priemonėmis galima sužinoti Centro duomenis ar kitaip sudaryti sąlygas susipažinti su Centro duomenimis.

67. Keitimosi informacija politika:

67.1. perduodant informaciją elektroniniu paštu, būtina:

67.1.1. atidžiai užrašyti adresato elektroninio pašto adresą, kad informacija nebūtų perduota kitam asmeniui;

67.1.2. už organizacijos ribų siunčiamiems laiškams naudoti el. pašto programoje numatytą el. laiško parašą ir jo nekeisti;

67.1.3. priimant sprendimus pagal elektroninio pašto 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;

67.2. neatverti pridėtų (ang. „attached“) failų, kurie yra gauti iš nepažįstamų asmenų, arba nėra galimybės įsitikinti šių failų turiniu;

67.3. už pašalinių asmenų naudojimąsi internetu kompiuteryje ir informacijos perdavimą elektroniniu paštu yra atsakingas kompiuterio naudotojas.

68. Apsaugos nuo virusų taisyklės:

68.1. prieš naudojant nežinomas išorines duomenų laikmenas arba kurios buvo naudojamos kitame kompiuteryje, būtina atlikti jų antivirusinę profilaktiką;

68.2. kilus įtarimui patikrinti kompiuterį nuo virusų;

68.3. 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 IT specialistą, tiesioginį vadovą arba Centro vadovą.

69. Jeigu Centro darbuotojas abejoja įdiegtų saugumo priemonių patikimumu, jis turi kreiptis į IT specialistą arba tiesioginį vadovą, kad būtų įvertintos turimos saugumo priemonės ir, jei reikia, inicijuotas papildomų priemonių įsigijimas ir įdiegimas.

70. Už asmens duomenų saugumo pažeidimų valdymą ir reagavimą į šiuos pažeidimus atsako Centro direktorius.

71. Asmens duomenų tvarkymo ir saugojimo įgyvendinimo priemonių sąrašas:

1. Fizinė prieiga prie kompiuterinės įrangos:
1.1. patalpos rakinamos;
1.2. veikia asmenų įėjimo į patalpas kontrolės sistema (fizinė).
2. Programinės įrangos naudotojai:
2.1. nustatyta naudotojų prieigos teisių suteikimo tvarka;
2.2. valdoma naudotojų teisė naudotis programine įranga;
2.3. registruojama informacija apie paskutinius informacinių sistemų ir jose esančių duomenų pakeitimus, juos atlikusius naudotojus, ir pakeitimų laiką.
3. Prieiga prie vidinio tinklo:
3.1. vidinis tinklas apsaugotas ugniasiene;
3.2. nutolę įrenginiai prie vidinio tinklo jungiasi saugiu ryšio kanalu (VPN, skirtinėmis linijomis ir pan.);
3.3. kontroliuojama naudotojų prieiga prie vidinio tinklo;
3.4. tinklu siunčiama informacija šifruojama.
4. Atsarginių duomenų kopijų ir laikmenų naudojimas:
4.1. atsarginės duomenų kopijos saugomos atskirose fizinėse laikmenose;
4.2. atsarginės duomenų kopijos ir laikmenos yra šifruojamos.
5. Apsauga nuo vagystės:
5.1. apribota fizinė prieiga prie tarnybinių stočių ir kompiuterinių darbo vietų;
5.2. apribota programinė prieiga prie tarnybinių stočių, kompiuterinių darbo vietų ir jose esančių duomenų;

6. Apsauga nuo piktnaudžiavimo duomenų perdavimo tinklu:
6.1. nustatyti griežti duomenų perdavimo tinklo srauto apribojimai.
7. **Programinės įrangos klaidos:**
7.1. naudojama legali programinė įranga, kuri prižiūrima laikantis gamintojo reikalavimų;
7.2. diegiami operacinių sistemų ir naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;
7.3. veikia informacinių sistemų infrastruktūros stebėjimo sistema.
8. Apsauga nuo kenkėjiškos programinės įrangos:
8.1. kompiuterinėse darbo vietose įdiegta antivirusinė programinė įranga;
8.2. darbuotojai supažindinti su vidaus tvarkomis ir žino, kaip elgtis pastebėjus kenkėjišką programinę įrangą.
9. Duomenų atstatymo gebėjimai:
9.1. numatyta duomenų atstatymo iš atsarginių kopijų procedūra.
10. Programinės įrangos naudojimas:
10.1. naudojama tik legali ir leistina programinė įranga;
10.2. nuolat atliekama kompiuterinėse darbo vietose naudojamos programinės įrangos kontrolė;
10.3. naudotojai patys negali diegti programinės įrangos.
11. Naudotojų švietimas:
11.1. naudotojai mokomi dirbti su programine įranga;
11.2. naudotojams parengtos tikslios ir išsamios darbo instrukcijos.
12. Apsauga nuo duomenų perdavimo tinklo įrangos gedimų:
12.1. įranga prižiūrima pagal gamintojo rekomendacijas;
12.2. priežiūrą ir gedimų šalinimą atlieka kvalifikuoti specialistai.
13. Apsauga nuo kompiuterinės įrangos gedimų:
13.1. įranga prižiūrima pagal gamintojo rekomendacijas;
13.2. priežiūrą ir gedimų šalinimą atlieka kvalifikuoti specialistai;
13.3. svarbiausios kompiuterinės įrangos techninė būklė nuolat stebima.
14. Apsauga nuo gaisro:
14.1. patalpose yra ugnies gesintuvai.
15. Apsauga nuo elektros srovės tiekimo sutrikimų:
15.1. svarbiausiai kompiuterinei įrangai skirti nenutrūkstamo maitinimo šaltiniai (UPS).
16. Apsauga nuo maitinimo ir ryšio linijų gedimų:
16.1. kabeliai yra izoliaciniuose vamzdžiuose;
16.2. elektros ir duomenų kabeliai saugiai atskirti.

VII SKYRIUS
BENDROSIOS DARBUOTOJŲ PAREIGOS DUOMENŲ APSAUGOS SRITYJE

72. Bendrosios darbuotojų pareigos:

72.1. kiekvienas darbuotojas, vykdydamas pareigas, susijusias su asmens duomenų tvarkymu, privalo laikytis šių Taisyklių, BDAR ir kitų teisės aktų, reglamentuojančių asmens duomenų apsaugą;

72.2. darbuotojai turi tvarkyti asmens duomenis taip, kad būtų laikomasi BDAR reikalavimų ir užtikrinamas tinkamas duomenų saugumas.

73. Asmens duomenų tvarkymas darbo funkcijų vykdymo metu:

73.1. darbuotojai privalo tvarkyti asmens duomenis tik tiek, kiek tai būtina jų darbo funkcijoms atlikti, ir tik pagal nustatytus tikslus, nurodytus Centro vidaus dokumentuose ar direktoriaus nurodymu;

73.2. prieš perduodant asmens duomenis tretiesiems asmenims, darbuotojas privalo įsitikinti, kad toks perdavimas yra teisėtas ir būtinas, laikantis duomenų tvarkymo veiklos įrašuose nurodytų tikslų.

74. Konfidencialumo ir saugumo užtikrinimas:

74.1. darbuotojai, turintys prieigą prie asmens duomenų, privalo laikytis konfidencialumo principo ir užtikrinti, kad su asmens duomenimis nesusipažintų neįgalioti asmenys;

74.2. darbuotojai privalo užtikrinti, kad asmens duomenys nebūtų saugomi jiems priklausančiose asmeninėse laikmenose ar įrenginiuose (pvz., asmeninėse atmintinėse, kompiuteriuose), nebent tam būtų gautas Centro leidimas. Tokiu atveju būtina naudoti papildomas apsaugos priemones, kad užtikrintų BDAR standartus (pvz., slaptažodžius, duomenų šifravimą);

74.3. darbuotojai turi laikytis švaraus stalo politikos, užtikrinančios, kad su asmens duomenimis susiję dokumentai nebūtų palikti viešose ar nesaugiose vietose.

75. Pranešimo apie duomenų saugumo pažeidimus tvarka:

75.1. darbuotojai privalo nedelsdami pranešti Centro direktoriaus pavaduotojui infrastruktūrai arba duomenų apsaugos pareigūnui apie bet kokius įtartinus veiksmus, incidentus ar pažeidimus, kurie gali kelti grėsmę duomenų saugumui;

75.2. pranešimo apie pažeidimą tikslas – kuo skubiau identifikuoti ir pašalinti pažeidimo šaltinį, todėl darbuotojai privalo informuoti atsakingus asmenis ne vėliau kaip per vieną darbo dieną nuo incidento pastebėjimo. Jei pranešti tiesiogiai neįmanoma, privaloma naudoti kitą Centrui prieinamą ryšio būdą;

75.3. darbuotojai turi bendradarbiauti su Centro vadovybe ir duomenų apsaugos pareigūnu, kad būtų atliktas pažeidimo tyrimas, imtasi tinkamų veiksmų ir prireikus – informuoti duomenų subjektai bei priežiūros institucijos.

76. Darbuotojų konsultavimas:

76.1. darbuotojai, turintys klausimų ar susidūrę su neaiškumais dėl asmens duomenų apsaugos, privalo kreiptis į duomenų apsaugos pareigūną arba kitą Centro įgaliotą asmenį, siekdami išvengti galimų pažeidimų.

VIII SKYRIUS
KANDIDATŲ Į DARBO VIETAS ASMENS DUOMENŲ TVARKYMAS

77. Centras atrankos į laisvas darbo vietas tikslais tvarko kandidatų asmens duomenis.

78. Kandidatai norintys tapti Centro darbuotojais, pateikia Centrui savo asmens duomenis. Konkurso ar atrankos proceso metu Centras tvarko kandidatų asmens duomenis nustatyta tvarka ir užtikrina šių duomenų saugumą.

79. Kandidatų asmens duomenų tvarkymo tikslas – Centro konkurso ar atrankos į laisvas darbo vietas vykdymas. Šiuo tikslu Centras renka, analizuoja, saugo ir kitaip tvarko kandidatų asmens duomenis rašytine bei elektronine forma.

80. Kandidatų asmens duomenų tvarkymo tikslas apima:

80.1. kandidato kvalifikacijos, kompetencijos nustatymas ir tinkamumo vertinimas;

80.2. kandidato profesinės (darbinės) patirties nustatymas ir tinkamumo vertinimas;

80.3. kandidato asmeninių dalykinių savybių nustatymas ir tinkamumo vertinimas;

80.4. darbo sutarties (paslaugų/darbo/praktikos) sudarymo formavimas ir pateikimas kandidatui.

81. Teisėtas kandidatų asmens duomenų tvarkymo nurodytu tikslu pagrindas – kandidato sutikimas (sutikimas laikomas duotu, kai kandidatas Centrui pateikia reikiamus dokumentus konkursui ar atrankai).

82. Centras be kandidato išankstinio sutikimo jo asmens duomenų neperduoda jokiems tretiesiems asmenims, išskyrus žemiau nurodytus atvejus.

83. Centre tvarkomi kandidatų pateikti asmens duomenys:

83.1. bendriniai asmens duomenys: vardas, pavardė, asmens kodas, pilietybė;

83.2. kontaktiniai duomenys: adresas, telefono Nr., el. paštas;

83.3. kvalifikaciniai ir darbo patirties duomenys: gyvenimo aprašymas, profesinės (darbinės) patirties duomenys, kvalifikacijos, profesinių įgūdžių, išsilavinimo duomenys, diplomai, sertifikatai, rašytinės rekomendacijos ir jose esantys duomenys;

83.4. kiti kandidato laisva valia pateikti asmens duomenys (duomenų pateikimas nėra būtinas, kandidatas duomenis pateikia laisva valia).

84. Centras renka asmens duomenis tiesiogiai iš kandidatų.

85. Centras tvarko (saugo) kandidatų asmens duomenis 5 darbo dienas po to, kai su atrinktu kandidatu bus pasirašyta darbo sutartis ir 1 metus jeigu to pageidavo kandidatas ir davė raštišką sutikimą (Taisyklių 3 priedas).

86. Centras imasi reikalingų techninių ir organizacinių priemonių, apsaugančių Kandidatų asmens duomenis nuo neteisėto tvarkymo ir/ar praradimo.

87. Įgyvendinant saugojimo termino apribojimo principą, asmens duomenys ištrinami ne tik iš elektroninės pašto dėžutės, bet ir kitų elektroninių resursų (pavyzdžiui, jei buvo teikiami per darbdavio informacinius išteklius ar buvo išsaugoti kompiuteryje ar serveryje), taip pat sunaikinamos popierinės jų kopijos.

IX SKYRIUS
DUOMENŲ SUBJEKTŲ TEISIŲ ĮGYVENDINIMAS

88. Centras užtikrina duomenų subjektų teisių, įtvirtintų Bendrojo duomenų apsaugos reglamento (ES) Nr. 2016/679, įgyvendinimą.

89. Duomenų subjektų teisių įgyvendinimas vykdomas vadovaujantis Šiaulių technologijų mokymo centro duomenų subjektų teisių įgyvendinimo tvarkos aprašu (toliau – Aprašas), patvirtintu Centro direktoriaus įsakymu. Aprašas reglamentuoja prašymų priėmimo, nagrinėjimo ir atsakymų pateikimo procedūras.

90. Duomenų subjektų prašymų valdymą vykdo Centro direktorius arba jo įgaliotas asmuo pagal Apraše nustatytą tvarką. Centro darbuotojas, gavęs asmens prašymą dėl jo asmens duomenų, informuoja direktorių arba įgaliotą asmenį per vieną darbo dieną, nebent dėl objektyvių priežasčių tai nėra įmanoma.

91. Duomenų subjektų prašymai nagrinėjami ir atsakymas teikiamas Apraše nustatytais terminais. Centro direktorius turi teisę pratęsti atsakymo terminą iki 60 dienų, jei to paties asmens prašymų kiekis ar sudėtingumas reikalauja daugiau laiko, apie tai informuojant duomenų subjektą.

92. Centro direktorius arba įgaliotas darbuotojas gali atsisakyti nagrinėti duomenų subjekto prašymą Apraše nustatytais atvejais, kai prašymas neatitinka teisės aktų reikalavimų arba yra nepagrįstas.

93. Centras užtikrina, kad asmenims būtų pateikiama tik ta informacija, kuri tiesiogiai susijusi su jų asmens duomenimis, vadovaujantis Aprašu ir taikytinais teisės aktais.

X SKYRIUS
TVARKOMŲ ASMENS DUOMENŲ INVENTORIZACIJA

94. Inventorizacijos tikslas, nustatyti ir dokumentuoti visus Centre tvarkomus asmens duomenis, jų tvarkymo tikslus, teisinius pagrindus ir kitus svarbius aspektus, siekiant užtikrinti duomenų tvarkymo teisėtumą ir atitiktį Bendrojo duomenų apsaugos reglamento (BDAR) reikalavimams.

95. Atsakingi asmenys:

95.1. duomenų apsaugos pareigūnas – atsakingas už inventorizacijos proceso organizavimą ir priežiūrą;

95.2. struktūrinių padalinių vadovai – atsakingi už tvarkomų asmens duomenų pateikimą ir inventorizacijos informacijos atnaujinimą.

96. Inventorizacijos vykdymo tvarka:

96.1. duomenų rinkimas: kiekvienas struktūrinis padalinys duomenų apsaugos pareigūnui turi pateikti informaciją apie tvarkomus asmens duomenis, įskaitant duomenų kategorijas, tvarkymo tikslus, teisinį pagrindą, duomenų subjektų grupes, duomenų saugojimo terminus ir perdavimus trečiosioms šalims;

96.2. informacijos dokumentavimas: gavęs informaciją iš struktūrinių padalinių, DAP atsakingas už jos suvedimą į vieną bendrą inventorizacijos sąrašo formą (Taisyklių 11 priedas);

96.3. inventorizacija peržiūrima ir atnaujinama iš karto po esminių duomenų tvarkymo pokyčių.

97. Inventorizacijos rezultatų peržiūra:

97.1. duomenų apsaugos pareigūnas peržiūri inventorizacijos rezultatus, siekiant užtikrinti, kad visi asmens duomenys yra tvarkomi teisėtai ir atitinka BDAR reikalavimus.

97.2. kiekvienas struktūrinis padalinys atsakingas už savo pateiktos informacijos tikslumą ir aktualumą.

98. Jei inventorizacijos metu nustatomi trūkumai ar neatitikimai, DAP pateikia rekomendacijas dėl jų šalinimo ir nurodo atsakingus asmenis bei terminus.

99. Visi inventorizacijos dokumentai turi būti saugomi taip, kad būtų užtikrintas jų konfidencialumas, vientisumas ir prieinamumas tik įgaliotiems asmenims.

100. Inventorizacijos dokumentai turi būti saugomi ne trumpiau kaip 5 metus arba ilgesnį laikotarpį, jei to reikalauja galiojantys teisės aktai.

XI SKYRIUS
DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI IR ATSAKYMŲ PATEIKIMAS Į PRIEŽIŪROS INSTITUCIJŲ PRAŠYMUS

101. Teisės aktų nustatytais atvejais, Centras privalo sudaryti ir tvarkyti veiklos įrašus, kurie būtini tam, kad Centras turėtų nuolatinę ir aktualią informaciją apie savo vykdomos duomenų tvarkymo veiklos apimtis, joje dalyvaujančius asmenis, naudojamas tvarkymo priemones.

102. Veiklos įrašuose yra Centro vidaus dokumentai, kuriuose gali būti konfidenciali informacija, todėl Veiklos įrašai negali būti viešinami ir turi būti saugomi kaip ir kita Centro konfidenciali informacija.

103. Atsakingi asmenys:

103.1. Duomenų apsaugos pareigūnas atsakingas už veiklos įrašų saugojimą ir priežiūrą;

103.2. struktūrinių skyrių vadovai atsakingi už informacijos apie vykdomą duomenų tvarkymą teikimą ir atnaujinimą.

104. Jei struktūrinio padalinio vadovas deleguoja šią užduotį kitam asmeniui, jis privalo užtikrinti, kad paskirtas asmuo turi reikiamus įgaliojimus ir žinias tinkamai atlikti šią užduotį.

105. Duomenų tvarkymo veiklos įrašų pildymo procesas:

105.1. informacijos surinkimas: kiekvienas struktūrinis padalinys pateikia informaciją apie jų vykdomą asmens duomenų tvarkymą: duomenų kategorijas, tvarkymo tikslus, teisinius pagrindus, duomenų subjektų grupes, duomenų gavėjus, duomenų saugojimo terminus ir saugumo priemones;

105.2. įrašų pildymas: surinkta informacija įtraukiama į veiklos įrašus, naudojant Centro patvirtintą veiklos įrašų formą (Taisyklių 9 priedas ir 10 priedas);

105.3. peržiūra ir atnaujinimas: veiklos įrašai turi būti reguliariai peržiūrimi, ypač kai atsiranda naujų duomenų tvarkymo procesų arba pasikeičia esami procesai. Atnaujinimus atlieka atsakingi struktūrinių padalinių vadovai arba paskirti asmenys, bendradarbiaudami su DAP;

105.4. patikra: DAP reguliariai atlieka veiklos įrašų patikrą, kad užtikrintų jų atitiktį BDAR ir kitų teisės aktų reikalavimus. Jei nustatomi neatitikimai, DAP pateikia rekomendacijas dėl jų pašalinimo.

106. Atsakymų pateikimas į priežiūros institucijų prašymus:

106.1. gavus priežiūros institucijos prašymą, Duomenų apsaugos pareigūnas nedelsdamas informuoja atsakingus struktūrinius padalinius, kurių duomenys gali būti susiję su prašymu;

106.2. atsakingi struktūriniai padaliniai pateikia reikiamą informaciją duomenų apsaugos pareigūnui per 3 darbo dienas nuo pranešimo gavimo;

106.3. Duomenų apsaugos pareigūnas surenka visą informaciją ir pateikia atsakymą priežiūros institucijai per nustatytą terminą, užtikrinant duomenų tikslumą ir išsamumą.

107. Veiklos įrašų saugojimas ir prieinamumas:

107.1. veiklos įrašai saugomi užtikrinant, kad jie būtų pasiekiami tik įgaliotiems asmenims;

107.2. prireikus, veiklos įrašai turi būti pateikiami priežiūros institucijoms ne vėliau kaip per 10 darbo dienų.

108. Veiklos įrašai turi būti saugomi ne trumpiau kaip 5 metus nuo duomenų tvarkymo proceso pabaigos arba ilgiau, jei tai numato teisės aktai arba Centro politika.

109. Visi Centro darbuotojai privalo suprasti veiklos įrašų svarbą ir savo atsakomybę už tinkamą jų pildymą bei saugojimą.

110. Veiklos įrašai yra tikrinami ir atnaujinami pagal poreikį, kad atitiktų realią asmens duomenų tvarkymo situaciją Centre. Už patikrą yra atsakingas duomenų apsaugos pareigūnas, jis įvertinęs patikrinimo rezultatus turi teisę inicijuoti vidaus auditą.

111. Veiklos įrašai viešai neskelbiami ir teikiami tik inspekcijai šios prašymu.

112. Duomenų apsaugos pareigūnas negali savarankiškai atnaujinti Veiklos įrašų, nesuderinęs to su atsakingais asmenimis, tačiau turėtų išreikšti nuomonę dėl atnaujinimo poreikio, jei mato priežastis, dėl kurių toks poreikis gali kilti (teisės aktų pasikeitimai, VDAI praktika, teismų praktika, kt.).

113. Veiklos įrašai yra tvarkomi raštu. Rašytinei formai yra prilyginama ir elektroninė forma, saugoma kompiuteryje.

XII SKYRIUS
POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

114. Poveikio duomenų apsaugai vertinimas (toliau – PDAV) – tai procesas, kurio metu vertinamas pavojus fizinių asmenų teisėms ir laisvėms, vertinant netinkamo duomenų valdymo ir jų praradimo įvykio tikimybę ir galimas pasekmes.

115. 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.

116. Centrui pradėjus vykdyti naują(-as) duomenų tvarkymo operaciją(-as), yra privaloma atlikti PDAV, jei duomenų tvarkymas:

116.1. 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 atpažinimas ir kt.);

116.2. automatizuotai būtų tvarkomi asmeniniai aspektai, vykdomas profiliavimas ir priimami teisiniai ar kiti didelio poveikio (pavyzdžiui, asmenų suskirstymas į grupes, kurios gali turėti jiems įtakos) sprendimai;

116.3. būtų pradėtas vykdyti sistemingas vaizdo stebėjimas dideliu mastu;

116.4. būtų pradėti tvarkyti specialių kategorijų asmens duomenys dideliu mastu.

117. PDAV taip pat gali būti atliekamas ir šiame skyriuje neaptartais atvejais, bet esant Centro vadovo sprendimu tai atlikti.

118. Vienas PDAV gali įvertinti keletą panašių tvarkymo operacijų, keliančių panašias dideles rizikas.

119. PDAV atlieka Centro vadovo įsakymu sudaroma darbo grupė ir Centro darbuotojų arba PDAV atlieka asmenys pagal paslaugų teikimo sutartį.

120. Centro vadovo įsakymu sudaromai darbo grupei paskiriamas jos vadovas atlikti PDAV. Į jos sudėtų gali būti įtrauktas ir duomenų apsaugos pareigūnas arba gali būti konsultuojamasi su duomenų apsaugos pareigūnu.

121. Darbo grupė PDAV metu pildo Priežiūros institucijos rekomenduojamą PDAV formą (Taisyklių 7 priedas).

122. Užpildyta ir pasirašyta forma teikiama Centro vadovui, kuris priima sprendimus dėl tolimesnio asmens duomenų tvarkymo.

123. Kai iš PDAV paaiškėja, kad duomenų tvarkymo operacijos kelia didelį pavojų duomenų subjektų teisėms ir laisvėms, o Centras 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.

124. Konsultavimasis su Priežiūros institucija atliekamas pagal Priežiūros institucijos nustatytą procedūrą ir reikalavimus.

XIII SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMAS

125. Šiame skyriuje išdėstytu asmens duomenų saugumo pažeidimo (toliau - Pažeidimas) valdymu (toliau – Procedūra) turėtų būti vadovaujamasi reaguojant į asmens duomenų saugumo pažeidimą, atsižvelgiant į konkrečios situacijos faktines aplinkybes.

126. Visi asmenys, turintys prieigą prie Centro tvarkomų asmens duomenų privalo žinoti ir vadovautis šia Procedūra Pažeidimo atveju.

127. Galimi šie Pažeidimai pagal pobūdį (tipą):

127.1. konfidencialumo pažeidimas – netyčia ar neteisėtai atskleidžiami asmens duomenys arba prie asmens duomenų suteikiama prieiga tam teisės neturintiems asmenims. Tokio pobūdžio pažeidimo pavyzdžiais galėtų būti asmens duomenų kopijos išsiuntimas trečiajam asmeniui, neturinčiam teisinio pagrindo juos gauti, prisijungimo prie duomenų bazės slaptažodžio paviešinimas ir pan.;

127.2. pasiekiamumo pažeidimas – netyčia ar neteisėtai prarandama prieiga prie asmens duomenų arba duomenys yra sunaikinami. Tokio pobūdžio pažeidimu galėtų būti duomenų bazės ištrynimas nesant atsarginės kopijos, iš kurios būtų galima atkurti prarastus duomenis. Pasiekiamumo pažeidimu, kuris turėtų būti aprašytas, būtų ir laikinas įprastinę Centro veiklą sutrikdęs prieigos prie asmens duomenų praradimas;

127.3. vientisumo pažeidimas – netyčia ar neteisėtai atliekami asmens duomenų pakeitimai. Tai galėtų būti trečiojo asmens, įgijusio neteisėtą prisijungimą prie duomenų bazės, įvykdyti joje esančių įrašų pakeitimai;

127.4. mišraus pobūdžio (tipo) pažeidimas – asmens duomenų konfidencialumo, prieinamumo ir vientisumo pažeidimas ar bet kurių aukščiau nurodytų pažeidimų derinys.

128. Pažeidimas gali įvykti dėl šių priežasčių:

128.1. 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.);

128.2. vagystė (pvz.: pavogti nešiojami / mobilūs įrenginiai, kuriuose saugomi asmens duomenys; pavogtos neautomatiniu būdu susistemintos bylos, kuriose yra asmens duomenų ir kt.);

128.3. 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.);

128.4. neleistina (neautorizuota) prieiga prie asmens duomenų (pvz.: įgaliojimų neturintys asmenys patenka į patalpas, kuriose saugomos bylos su asmens duomenimis; įgaliojimų neturintys asmenys prisijungia prie duomenų bazių ar informacinių sistemų ir kt.);

128.5. 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.);

128.6. nenumatytos (force majeure) aplinkybės ir kitos priežastys (gaisras, vandens užliejimas, dėl kurių sugadinami arba prarandami asmens duomenys ir kt.).

129.Centro darbuotojas, pastebėjęs, nustatęs, gavęs informaciją apie galimą Pažeidimą iš duomenų tvarkytojo ar kito šaltinio, privalo:

129.1. nedelsiant, bet ne vėliau kaip per 2 darbo valandas nuo galimo Pažeidimo paaiškėjimo momento informuoti žodžiu, raštu ar elektroninėmis priemonėmis Centro direktoriaus pavaduotoją infrastruktūrai ir Pareigūną;

129.2. užpildyti Pranešimą (Taisyklių 4 priedas) ir nedelsiant, bet ne vėliau kaip per 4 darbo valandas nuo galimo Pažeidimo paaiškėjimo momento perduoti jį Centro direktoriaus pavaduotojui infrastruktūrai, o jo kopiją – Pareigūnui;

129.3. jei įmanoma, imtis priemonių pašalinti galimą Pažeidimą ir imtis priemonių galimoms neigiamoms jo pasekmėms sumažinti.

130. Centro direktoriaus pavaduotojas infrastruktūrai, gavęs Pranešimą apie Pažeidimą, privalo:

130.1. atlikti Pažeidimo tyrimą ir nedelsdamas, bet ne vėliau kaip per 24 valandas nuo Pranešimo gavimo momento nagrinėti Pranešime nurodytas aplinkybes;

130.2. įvertinti, ar padarytas Pažeidimas;

130.3. konsultuotis su Pareigūnu;

130.4. jei Pažeidimas yra susijęs su elektroninės informacijos saugos incidentu, pasitelkti Centro ar duomenų tvarkytojo IT specialistus;

130.5. jei Pažeidimas padarytas, nustatyti, kokio pobūdžio (tipo) Pažeidimas padarytas, asmens duomenų, kurių saugumas pažeistas, kategorijas, įskaitant specialių kategorijų asmens duomenis, Pažeidimo priežastis, Pažeidimo apimtis (duomenų subjektų kategorijos ir jų skaičius), 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 (toliau – Ataskaita) (Taisyklių 5 priedas) dėl pažeidimo buvimo ir rizikos;

130.6. teikti rekomendacijas Centro 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;

130.7. įvertinti, kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas Pažeidimas;

130.8. nustatyti, ar apie Pažeidimą būtina pranešti VDAI;

130.9. nustatyti, ar apie Pažeidimą būtina pranešti duomenų subjektams.

131. Pareigūnas, gavęs Pranešimą, privalo:

131.1. Centro direktoriaus pavaduotojui infrastruktūrai patarti dėl Pažeidimo tyrimo ir teikti išvadas dėl Pranešimo teikimo VDAI ir (ar) duomenų subjektui;

131.2. bendradarbiauti su VDAI dėl pažeidimų.

132. Atliekant Pažeidimo tyrimą ir siekiant nustatyti, ar Pažeidimas iš tikrųjų įvyko, esamos situacijos įrodymai privalo būti fiksuojami dokumentuose ir užtikrinamas jų atsekamumas.

133. Pažeidimo tyrimo metu darbuotojai ir duomenų tvarkytojas privalo operatyviai teikti Centro direktoriaus pavaduotojui infrastruktūrai visą jo paprašytą su Pažeidimu susijusią informaciją ir dokumentus.

134. Vertinant rizikos lygį, atsižvelgiama į konkrečias pažeidimo aplinkybes, pavojaus duomenų subjektų teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizikos lygis vertinamas atsižvelgiant į šiuos kriterijus:

134.1. saugumo pažeidimo pobūdis (konfidencialumo, vientisumo ar prieinamumo pažeidimas) – nustatomas saugumo pažeidimo pobūdis: nuo padaryto pažeidimo pobūdžio gali priklausyti pavojaus duomenų subjektams dydis;

134.2. asmens duomenų pobūdis, jautrumas ir kiekis – nustatomas asmens duomenų, kurių saugumas buvo pažeistas, pobūdis, jautrumas ir jų kiekis: kuo jautresni asmens duomenys ir kuo didesnis jų kiekis, tuo didesnis žalos pavojus;

134.3. galimybė identifikuoti fizinį asmenį – įvertinama, ar neįgaliotiems asmenims, kuriems tapo prieinami asmens duomenys, bus lengva nustatyti konkrečių asmenų tapatybę arba susieti tuos duomenis su kita informacija (pvz., tinkamai užšifruoti asmens duomenys nebus suprantami neįgaliotiems asmenims, todėl pažeidimas padarys mažesnį poveikį duomenų subjektams);

134.4. fizinio asmens specifiniai ypatumai – nustatomi fizinių asmenų, kurių asmens duomenims kilo pavojus, specifiniai ypatumai: kuo asmenys yra labiau pažeidžiami (pvz., vaikai, negalią turintys asmenys), tuo didesnį poveikį pažeidimas gali jiems padaryti;

134.5. nukentėjusių duomenų subjektų skaičius – nustatomas nukentėjusių asmenų skaičius: kuo daugiau yra asmenų, kuriems pažeidimas turi poveikio, tuo didesnis žalos pavojus;

134.6. pasekmės, sukeltos fiziniams asmenims – įvertinamos visos galimos pažeidimo pasekmės bei jų rimtumas; taip pat atsižvelgiama į pasekmių ilgalaikiškumą: jei pažeidimo pasekmės yra ilgalaikės, tai poveikis fiziniams asmenims bus didesnis.

135. Įvertinus riziką nustatomas vienas iš trijų rizikos tikimybių lygių – maža, vidutinė ar didelė rizikos tikimybė.

136. Ataskaita yra pateikiama Centro direktoriui ir duomenų tvarkytojo vadovui, jei tai susiję su duomenų tvarkytojo atliekamais asmens duomenų tvarkymo veiksmais.

137. Atsižvelgiant į Ataskaitą, Centro direktorius, jei reikia, tvirtina priemonių planą, kuriame numatomas būtinų techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl Pažeidimo pašalinimo, paskiria atsakingus vykdytojus ir nustato priemonių įgyvendinimo terminus.

138. Sprendžiant Pažeidimo pašalinimo klausimą, bei tvirtinant priemonių planą, pirmiausia būtina atlikti veiksmus, siekiant apriboti ar sustabdyti saugumo incidentą. Priklausomai nuo konkrečių Pažeidimo aplinkybių, turėtų būti atlikti tokie veiksmai, kaip: ištrinti asmens duomenis nuotoliniu būdu iš pamesto ar pavogto nešiojamo/mobilaus įrenginio (telefono, nešiojamo kompiuterio ir kt.); jei asmens duomenys per klaidą išsiunčiami ne tam adresatui, kuriam jie buvo skirti, kuo skubiau kreiptis į jį su prašymu ištrinti atsiųstus asmens duomenis be galimybės juos atkurti; pakeisti prisijungimo prie duomenų bazės ar informacinės sistemos vardus ir slaptažodžius, jeigu jie tapo žinomi tretiesiems asmenims; atkuriant prarastus ar sugadintus asmens duomenis, naudoti atsargines kopijas ir kt.

139. Siekiant apriboti ar sustabdyti Pažeidimą, būtina kiek įmanoma tiksliau surinkti duomenų ir įrodymų apie įvykusį saugumo incidentą (pvz., kas, kada ir iš kokio įrenginio jungėsi prie duomenų bazės ar informacinės sistemos, kam per klaidą išsiųsti asmens duomenys, kokiomis aplinkybėmis buvo prarastas įrenginys su asmens duomenimis ir kt.).

140. Priemonių plane turi būti numatyti veiksmai, nukreipti ne vien į esamo Pažeidimo priežasties pašalinimą, pavojaus fizinių asmenų teisėms ir laisvėms sumažinimą ar pašalinimą, bet taip pat skirti neleisti pasikartoti Pažeidimui. Būtina atsižvelgti į trūkumus ir duomenų tvarkymo silpnąsias vietas, kurios buvo išnaudotos įvykdant Pažeidimą bei imtis priemonių tuos trūkumus pašalinti.

141. Tyrimo metu nustačius, kad Pažeidimas buvo, Centro direktoriui priėmus sprendimą dėl Pranešimo priežiūros institucijai pateikimo būtinybės, Centro direktoriaus įgaliotas darbuotojas privalo nedelsiant, bet ne vėliau nei kaip per 72 val. nuo tada, kai tapo žinoma apie Pažeidimą, apie tai informuoti VDAI (Taisyklių 6 priedas), išskyrus atvejus, kai Pažeidimas nekelia pavojaus fizinių asmenų teisėms ir laisvėms.

142. Jeigu įvertinus riziką, abejojama, ar Pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, apie pažeidimą pranešama VDAI.

143. Jeigu po pranešimo VDAI pateikimo, atlikus tolesnį tyrimą, yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai Pažeidimo nebuvo, apie tai nedelsiant informuojama VDAI.

144. Tyrimo metu nustačius, kad dėl Pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, Centro direktoriaus pavaduotojas infrastruktūrai 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.

145. Duomenų subjektas informuojamas tiesiogiai, t. y. siunčiant jam pranešimą paštu, elektroniniu paštu, trumpąja žinute (SMS) ar kitu būdu. Pranešimas duomenų subjektui siunčiamas atskirai nuo kitos siunčiamos informacijos, kaip naujienlaiškiai ar standartiniai pranešimai.

146. Pagrindinis pranešimo duomenų subjektui tikslas – pateikti konkrečią informaciją apie tai, kokių veiksmų jis turėtų imtis, kad apsisaugotų nuo neigiamų pažeidimo pasekmių. Pranešime duomenų subjektui aiškia ir paprasta kalba pateikiama ši informacija:

146.1. asmens duomenų saugumo pažeidimo pobūdžio ir tikėtinų pažeidimo pasekmių aprašymas;

146.2. priemonės, kurių ėmėsi Centras, kad būtų pašalintas saugumo pažeidimas;

146.3. Pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, kontaktiniai duomenys;

146.4. kita reikšminga informacija, susijusi su pažeidimu, kuri, Centro direktoriaus pavaduotojo infrastruktūrai manymu, turėtų būti pateikta duomenų subjektui, pvz., patarimai, kaip apsisaugoti nuo galimų neigiamų pažeidimo pasekmių.

147. Pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta Valstybinei duomenų apsaugos inspekcijai, ar ne, registruojami Asmens duomenų saugumo pažeidimų registravimo žurnale (toliau – Žurnalas) (Taisyklių 12 priedas).

XIV SKYRIUS
DARBUOTOJŲ MOKYMAS

148. Visiems į darbą Centre priimtiems darbuotojams pirmosiomis jų darbo Centre dienomis yra vedami mokymai su Centre tvarkomų asmens duomenų procesais. Mokymai apima, bet neapsiriboja supažindinimu su šiomis Taisyklėmis, po supažindinimo kiekvienas darbuotojas, kuris savo darbinėje veikloje tvarkys asmens duomenis, pasirašo Konfidencialumo įsipareigojimą, darbuotojas taip pat supažindinamas su Centro kitais vidaus tvarkos dokumentais, kurie yra susiję su elgesio internetinėje erdvėje, techninėmis ir administracinėmis priemonėmis, kurių turi imtis kiekvienas konkretus darbuotojas pagal jo pareigybes ir kita susijusia informacija bei gerąją praktika. Mokymai, be kita ko, apima ir pagrindinių sąvokų (duomenų valdytojas, duomenų tvarkytojas, duomenų subjektas, asmens duomenys, duomenų tvarkymas, specialių kategorijų asmens duomenys) bei esminių reikalavimų asmens duomenų tvarkymui išaiškinimą.

149. Mokymai turėtų atitikti darbuotojų veiklos realijas.

150. Mokymų turinys turi padėti darbuotojams vykdyti savo darbines pareigas laikantis Reglamento ir kituose asmens duomenų apsaugą reglamentuojančiuose teisės aktuose nustatytų reikalavimų.

151. Mokymus organizuoja Centro direktorius arba duomenų apsaugos pareigūnas.

152. Mokymai yra dokumentuojami, nurodant jų datą, temą ir dalyvavusius darbuotojus.

XV SKYRIUS
DUOMENŲ APSAUGOS PAREIGŪNAS

153. Centre yra paskirtas duomenų apsaugos pareigūnas.

154. Pareigūno kontaktiniai duomenys skelbiami Centro internetinėje svetainėje duomenų subjektas lengvai prieinamoje vietoje, tam skirtoje skiltyje „Asmens duomenų apsauga“.

155. Pareigūnas privalo:

155.1. užtikrinti, kad Centre 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;

155.2. stebėti, kaip laikomasi BDAR, kitų asmens duomenų teisinę apsaugą reglamentuojančių teisės aktų reikalavimų, šių Taisyklių, kitų vidinių dokumentų, susijusių su asmens duomenų apsauga;

155.3. konsultuoti ir stebėti, kaip Centre atliekamas poveikio duomenų apsaugai vertinimas;

155.4. informuoti Centro vadovą ir kitus darbuotojus apie jų pareigas pagal BDAR ir kitus, asmens duomenų apsaugą reglamentuojančius, teisės aktus ir juos konsultuoti dėl konkrečių pareigų vykdymo;

155.5. informuoti Centro vadovą apie bet kokius neatitikimus, pažeidimus asmens duomenų apsaugos srityje, kuriuos, duomenų apsaugos pareigūnas nustato, vykdydamas savo funkcijas;

155.6. mokyti Centro darbuotojus, dirbančius su asmens duomenimis, asmens duomenų teisinės apsaugos klausimais;

155.7. bendradarbiauti, būti kontaktiniu asmeniu santykiuose su VDAI.

156. Duomenų apsaugos pareigūnas savo pareigas ir užduotis atlieka nepriklausomai. Centro vadovas, ir jokie kiti Centro darbuotojai duomenų apsaugos pareigūnui negali teikti jokių nurodymų dėl jo užduočių vykdymo.

157. Duomenų apsaugos pareigūnas turi teisę naudotis Centro personalo pagalba ir prašyti iš jų bet kokios informacijos, būtinos jo funkcijoms atlikti. Pareigūnui turi būti suteikta prieiga prie visų Centro vidinių dokumentų ir sistemų, susijusių su duomenų tvarkymu, siekiant tinkamai vykdyti jam pavestas užduotis, atsižvelgiant į taikomus konfidencialumo reikalavimus ir pareigūno atliekamo darbo pobūdį.

158. Vykdydamas savo pareigas, duomenų apsaugos pareigūnas vadovaujasi Reglamento, kitų, asmens duomenų tvarkymą reglamentuojančių, teisės aktų bei pareiginių nuostatų reikalavimais.

159. Duomenų apsaugos pareigūnas gali vykdyti ir kitas užduotis bei pareigas, Centrui užtikrinant, kad dėl tokių užduočių ir pareigų nekils interesų konfliktas.

160. Per 5 darbo dienas po duomenų apsaugos pareigūno išrinkimo arba pasikeitimo Centras privalo viešai paskelbti duomenų apsaugos pareigūno kontaktinius duomenis ir apie juos pranešti VDAI.

161. Duomenų apsaugos pareigūnas tiesiogiai atsiskaito Centro direktoriui.

162. Duomenų apsaugos pareigūnas negali būti atleistas arba baudžiamas dėl savo funkcijų vykdymo.

163. Duomenų apsaugos pareigūnas nėra asmeniškai atsakingas už Centro padarytus asmens duomenų tvarkymo pažeidimus, atsakomybė už pažeidimus bet kokiu atveju tenka Centrui.

XVI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

164. Taisyklės skelbiamos Šiaulių technologijų mokymo centro interneto svetainėje, skiltyje „Asmens duomenų apsauga“.

165. Centro darbuotojai su Taisyklėmis bei jos pakeitimais supažindinami pasirašytinai arba susipažįsta patvirtindami dokumentą duomenų valdymo sistemoje (DBSIS) ir privalo laikytis jose nustatytų įsipareigojimų bei atlikdami savo darbo funkcijas vadovautis Taisyklėse nustatytais principais. Priėmus naują darbuotoją jis su Taisyklėmis privalo susipažinti pirmąją jo darbo dieną.

166. Šiose Taisyklėse esančios nuostatos gali būti papildomos ar išsamiau įtvirtinamos kituose Centro veiklą reglamentuojančiuose vidaus dokumentuose. Rengiant vidaus dokumentus, visais atvejais turi būti vadovaujamasi Taisyklėmis. Jeigu duomenų apsaugos klausimais yra prieštaravimų tarp Taisyklių ir kitų Centro vidaus dokumentų, turi būti vadovaujamasi Taisyklių nuostatomis. Tuo atveju, jeigu klausimai, susiję su asmens duomenų apsauga nėra reglamentuoti Taisyklėse, turi būti taikomi kiti Centro vidaus dokumentai.

167. Centro darbuotojai, pažeidę Taisykles, ADTAĮ ir (ar) BDAR, atsako teisės aktų nustatyta tvarka.

168. Pasikeitus asmens duomenų tvarkymą reglamentuojantiems teisės aktams, Taisyklės yra peržiūrimo ir atnaujinamos.

169. Taisyklių priedai, jeigu tokių yra, tampa neatsiejama Šių Taisyklių dalimi.

Taisyklių priedai:
1 priedas Konfidencialumo įsipareigojimas
2 priedas Sutikimas dėl asmens duomenų tvarkymo
3 Priedas Kandidato sutikimas dėl asmens duomenų tvarkymo
4 Priedas Pranešimas apie asmens duomenų saugumo pažeidimą (Centro viduje)
5 priedas Asmens duomenų saugumo pažeidimo tyrimo ataskaita
6 Priedas Pranešimas apie asmens duomenų saugumo pažeidimą
7 Priedas Poveikio duomenų apsaugai vertinimo ataskaita
8 Priedas „Privacy by default“ ir „Privacy by design“ duomenų apsaugos principų taikymo gairės
9 Priedas Duomenų valdytojo duomenų tvarkymo veiklos įrašas
10 Priedas Duomenų tvarkytojo duomenų tvarkymo veiklos įrašas
11 Priedas Tvarkomų asmens duomenų inventorizacijos sąrašas
12 Priedas Asmens duomenų saugumo pažeidimų registravimo žurnalas

PRITARTA
Darbo tarybos 2024 m. lapkričio 7 d. protokolo Nr. DTV-5

Šiaulių technologijų mokymo centro
Asmens duomenų tvarkymo taisyklių
1 priedas

Šiaulių technologijų mokymo centro
direktoriui

KONFIDENCIALUMO ĮSIPAREIGOJIMAS

_____
(data)

Šiauliai

Aš, _____,
(vardas, pavardė)

_____,
(pareigos)

Žemiau pasirašydama (-as) patvirtinu, jog:

Aš suprantu:

- kad savo darbe tvarkysiu asmens duomenis (įskaitant ir specialių kategorijų duomenis), kurie negali būti atskleisti ar perduoti neįgaliotiems asmenims, įmonėms, įstaigoms ar institucijoms;
- kad draudžiama perduoti neįgaliotiems asmenims slaptažodžius ir kitus duomenis, leidžiančius programinių ir techninių priemonių pagalba sužinoti asmens duomenis ar kitaip sudaryti sąlygas susipažinti su asmens duomenimis;
- kad netinkamas asmens duomenų tvarkymas gali užtraukti atsakomybę pagal Lietuvos Respublikos įstatymus.

Aš įsipareigoju:

- saugoti asmens duomenų paslaptį;
- tvarkyti asmens duomenis vadovaudamasis Reglamentu, Lietuvos Respublikos įstatymais ir kitais teisės aktais, Asmens duomenų tvarkymo taisyklėmis, taip pat savo pareigybės aprašymu, reglamentuojančiu man patikėtas asmens duomenų tvarkymo funkcijas;
- neatskleisti informacijos ir neperduoti galimybės įvairiomis priemonėmis susipažinti su tvarkoma informacija nei vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija tiek Centro viduje, tiek už jo ribų;
- pranešti Centro direktoriui apie bet kokią įtartiną situaciją, kuri gali kelti grėsmę asmens duomenų saugumui;
- saugoti ir tik įstatymu bei kitų teisės aktų nustatyta tvarka naudoti asmens duomenis, kurie man taps žinomi atliekant savo darbo funkcijas.

Aš žinau:

- kad už šio įsipareigojimo nesilaikymą, ir Reglamento Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pažeidimą turėsiu atsakyti pagal galiojančius Lietuvos Respublikos įstatymus;
- kad asmuo, patyręs žalą dėl neteisėto asmens duomenų tvarkymo arba kitų duomenų valdytojo ar duomenų tvarkytojo veiksmų ar neveikimo, turi teisę reikalauti atlyginti jam padarytą turtinę ar neturtinę žalą;
- kad duomenų valdytojas, duomenų tvarkytojas arba kitas asmuo, atlyginęs asmeniui padarytą žalą, patirtą nuostolį išsireikalauja įstatymu nustatyta tvarka iš asmens duomenis tvarkančio darbuotojo, dėl kurio kaltės atsirado ši žala;
- kad asmens duomenis, kuriuos sužinosiu savo darbo Centre metu, turėsiu laikyti paslaptyje tiek visą mano darbo laiką šiame Centre, (nepriklausomai nuo pareigų pasikeitimo), tiek ir neribotą laiką pasibaigus darbo santykiams.

Taip pat patvirtinu, kad aš esu susipažinęs/-usi su Šiaulių technologijų mokymo centro Asmens duomenų tvarkymo taisyklėmis bei jų priedais.

_____
(parašas)

Šiaulių technologijų mokymo centro
Asmens duomenų tvarkymo taisyklių
2 priedas

Duomenų valdytojas:
Šiaulių technologijų mokymo centras
Kodas 306139052
Registruotos buveinės adresas: Dvaro g. 144A, LT-76199 Šiauliai

SUTIKIMAS DĖL ASMENS DUOMENŲ TVARKYMO

20.....-.....-.....
Šiauliai

Šis Sutikimas dėl asmens duomenų tvarkymo (toliau – Sutikimas) pasirašomas tarp **Šiaulių technologijų mokymo centro**, kaip darbdavio (toliau – Centras) ir Centro darbuotojų, siekiant įgyvendinti Bendrajame duomenų apsaugos reglamente (ES) 2016/679 (toliau – Reglamentas arba BDAR) numatytas priemones, skirtas asmens duomenų apsaugai. Vienas iš esminių Reglamento reikalavimų yra, kad asmens duomenų tvarkymas būtų grindžiamas pagrindiniais teisėtumo, sąžiningumo ir skaidrumo principais.

Atsižvelgiant į tai, jog Centro veikla yra paremta žmogiškaisiais ištekliais, Centras nuolatos įdarbina asmenis, su kuriais sukuriami darbdavio/darbuotojo santykiai, dėl ko Centrui, kaip darbdaviui, kyla pareiga tvarkyti Centrui suteikiamus asmens duomenis, o darbuotojui būtinybė suteikti Centrui asmens duomenis. Tam, kad toks duomenų tvarkymas iš Centro, kaip jam suteikiamų asmens duomenų valdytojo, pusės būtų teisėtas, yra reikalinga gauti asmens, kurio asmens duomenys yra tvarkomi, sutikimą tokius duomenis tvarkyti konkrečiai nustatytiems tikslams.

Todėl, siekiant įteisinti Centro teisę tvarkyti asmens duomenis ir galimybę tinkamai įgyvendinti jai įstatymu numatytą pareigą tvarkyti asmens duomenis darbdavio/darbuotojo santykiuose, o taip pat įtvirtinant darbuotojo teisę į tinkamą asmens duomenų apsaugą, pasirašomas šis darbuotojo Sutikimas, žemiau nurodytomis sąlygomis:

1. Asmuo, duodantis sutikimą tvarkyti duomenis*:

Darbuotojas (vardas, pavardė):	
Centre užimamos pareigos:	

**Asmens duomenis darbuotojas įrašo ranka*

2. Sutikimas tvarkyti asmens duomenis suteikiamas:

Darbdaviui:	**Šiaulių technologijų mokymo centras**
Juridinio asmens kodas:	306139052
Adresas:	Dvaro g. 144A, LT-76199 Šiauliai

3. Asmens duomenys tvarkomi šiais tikslais, kaip tai nurodyta BDAR 6 straipsnio 1 dalies b) ir c) punktuose:

6 straipsnio 1 dalies b) punkto apimtimi	Tvarkyti duomenis būtina siekiant įvykdyti sutartį, kurios šalys yra duomenų subjektas.
6 straipsnio 1 dalies c) punkto apimtimi	Tvarkyti duomenis būtina, kad būtų įvykdyta duomenų valdytojui taikoma teisinė prievolė.

4. Sutikimas teikiamas tvarkyti šiuos asmens duomenis, kaip tai apibrėžia BDAR 4 straipsnio 1 punkte:

Asmens duomenys:	Bet kokia informacija (identifikatoriai) apie fizinį asmenį (darbuotoją), kuria remiantis galima tiesiogiai arba netiesiogiai nustatyti asmens (darbuotojo) tapatybę, kaip antai – vardas, pavardė, asmens identifikavimo numeris, kontaktiniai duomenys, buvimo duomenys, atvaizdas, užimamos pareigos, šeimos narių duomenys (jei reikalinga pateikti pagal įstatymą), banko duomenys, jei tokius yra reikalinga nurodyti pasirašant darbo sutartį su Centru, ir pan.

5. Be asmens duomenų, nurodytų 4 Sutikimo punkte, ir asmens duomenų tvarkymo tikslų, nurodytų Sutikimo 3 punkte, Darbuotojas sutinka, kad jo asmens duomenys būtų tvarkomi šiais tikslais ir šiomis sąlygomis:*

1.	Atvaizdas	Fotografuojant ir/ar filmuojant Centro organizuojamus su Centro veikla susijusius renginius, susitikimus, taip pat pramoginius renginius, talpinant tokią vaizdo medžiagą į Centro failų serverį (su teise tik peržiūrėti tokią medžiagą ir tik Centro darbuotojams), su teise tokią vaizdo medžiagą naudoti Centro viduje (pvz.: puošiant Centro patalpas, persiunčiant vaizdo medžiagą išskirtinai tik Centro viduje). Bet koks kitas išorinis tokios vaizdo medžiagos viešinimas negalimas be atskiro sutikimo. Duomenys saugomi 2 metus.	Sutinku / Nesutinku _____ parašas
		Fotografuojant ir/ar filmuojant Centro ir kitų organizuojamus su Centro veikla susijusius renginius, susitikimus, taip pat pramoginius renginius ir kt., talpinant tokią vaizdo medžiagą į Centro failų serverį (su teise viešinti tokią medžiagą), su teise tokią vaizdo medžiagą naudoti Centro komunikacijai, reklamai, žinomumui didinti ir kt. (pvz.: ruošiant reklaminius lankstinukus, viešinant Centro veiklas žiniasklaidoje, soc. tinkluose, reklaminiuose stenduose ir kt.). Duomenys saugomi 2 metus.	Sutinku / Nesutinku _____ parašas
2.	Asmeninis elektroninis paštas	Asmens duomenis naudoti siekiant persiųsti darbuotojui aktualią informaciją, susijusią su darbine veikla.	Sutinku / Nesutinku _____ parašas
3.	Asmeninis telefono numeris	Asmens duomenis naudoti komunikacijai su darbuotoju palaikyti.	Sutinku / Nesutinku _____ parašas
4.	Sveikinimas su gimtadieniu ir amžiaus atskleidimas	Asmens duomenis naudoti siekiant pasveikinti su gimimo diena.	Sutinku / Nesutinku _____ parašas

***Apibraukti ,,Sutinku“ arba ,,Nesutinku“, apibraukus norimą terminą, pasirašyti po kiekvienu punktu nurodytoje vietoje.*

6. Darbuotojas yra informuotas, kad teisinės prievolės bei teisėtų Centro interesų pagrindu asmens duomenis gali gauti šie asmens duomenų gavėjai:

Duomenų gavėjai:	- Centro darbuotojai, kurie yra atsakingi už atitinkamų darbuotojų asmens duomenų tvarkymą (personalo, apskaitos, informacinių technologijų, atitinkamai jiems priskirti ir vykdomai funkcijai arba šių asmens duomenų tvarkymo paslaugą atliekančios įmonės); - Informacinių sistemų, kurias Centras naudoja Centro veiklos valdymui, teikėjai ir prižiūrėtojai; - Valstybinės institucijos, kurioms Centras turi prievolę teikti asmens duomenis (pvz.: Valstybinė mokesčių inspekcija, SoDra ir pan.); - Banko įstaigos (pvz.: atliekant pavedimą, kai yra mokamas atlyginimas); - Kiti asmenys, kuriems Centras turi prievolę teikti Darbuotojo asmens duomenis.	parašas

7. Asmens duomenų saugojimo terminai:

jei kitaip nenurodyta Sutikime, asmens duomenys saugomi Centre tiek, kiek tai leidžia darbuotojo/darbdavio santykius reglamentuojantys teisės aktai (įskaitant, bent neapsiribojant, LR Darbo kodeksu, Lietuvos vyriausiojo archyvaro 2014 m. lapkričio 6 d. Įsakymo Nr.(1.3E) VE-52 redakcija).

8. Taikymas:

šio Sutikimo sąlygos pradedamos taikyti nuo _____ d. iki šios datos Centro tvarkytiems Darbuotojo asmens duomenims Sutikimo sąlygos netaikomos.

9. Man yra žinoma, kad aš turiu teisę:

9.1. būti informuotas apie savo asmens duomenų tvarkymą;
9.2. susipažinti su tvarkomais mano asmens duomenimis ir žinoti, kaip jie yra tvarkomi;
9.3. reikalauti ištaisyti neteisingus, neišsamius, netikslius savo asmens duomenis;
9.4. nesutikti (pareiškiant nesutikimą raštu), kad būtų tvarkomi mano asmens duomenys;
9.5. pateikti skundą Valstybinei duomenų apsaugos inspekcijai.

10. Patvirtinu, kad:

10.1. esu informuotas, kad turiu teisę atšaukti šį savo duotą sutikimą (visą ar iš dalies) bet kuriuo metu, informuodamas apie tai Centrą raštu bei siunčiant pasirašytą kokybišką skenuotą Sutikimo atšaukimo kopiją el. paštu: personalas@stmc.lt;

10.2. man yra žinomos kitos mano, kaip duomenų subjekto, teisės, nustatytos 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB ir kituose asmens duomenų apsaugą reglamentuojančiuose teisės aktuose;

10.3. Centras mane tinkamai ir visapusiškai supažindino su šio Sutikimo davimo tikslu, galimomis pasekmėmis, mano teisėmis.

_____

Sutikimą suteikiančio darbuotojo parašas, vardas, pavardė ir data

Patvirtinu, kad visi toliau pateikti duomenys yra teisingi, ir įsipareigoju, pasikeitus bet kuriam iš šių duomenų, apie tai pranešti darbdaviui bei pataisyti šią anketą.

DARBUOTOJO ANKETA														
I. Darbuotojo asmens duomenys														
1.	Vardas													
2.	Pavardė													
3.	Asmens kodas											Gimimo data		
4.	Asmens dokumento (paso, kortelės) Nr.													
5.	Asmens dokumento išdavimo data ir galiojimo data													
6.	*Neįgaliojo pažymėjimo Nr.													
7.	*Neįgaliojo pažymėjimo galiojimo data													
8.	*Neįgalumo arba turimo darbingumo lygis													
	*(*pildo asmuo turintis negalią)*													

II. Adresai

Gyvenamosios vietos adresas (ne registracijos/deklaruojamas, bet kur tikrai gyvenate)		
9.	Gatvės pavadinimas, namo Nr., buto Nr., miestas (kaimas), rajonas	
10.	Mobilaus telefono (jeigu turite) Nr.	
11.	Asmeninio elektroninio pašto adresas	
Asmuo, kuriam pranešti, jeigu Jums darbe atsitiko nelaimė, ar kitu ypatingu atveju		
12.	Asmens vardas, pavardė	
13.	Asmens telefono Nr.	

III. Išsilavinimas

14.	Vidurinis/profesinis/aukštesnysis/aukštasis (įrašyti tinkamą žodį)	
15.	Mokslo įstaigos pavadinimas	
16.	Specializacija (specialybė)	
17.	Laipsnis (bakalauras, magistras, kt.)	
18.	Mokslo pabaigimo data	
19.	Mokslo įstaigos pavadinimas	
20.	Specializacija (specialybė)	
21.	Laipsnis	
22.	Mokslo pabaigimo data	

IV. Duomenys apie šeimos narius

23.	Šeimyninė padėtis		
24.	Ar turite nepilnamečių vaikų (globotinių)?	Taip	Ne
25.	Ar vaiką (vaikus) auginate vienas?	Taip	Ne
	Informacija apie vaikus *(pildyti, jei auginate vaiką iki 14 m. ar neįgalų vaiką iki 18 m.)*		
26.	Gimimo data (metai, mėnuo, diena)	1.	
27.	Vardas, pavardė		
28.	Neįgaliojo pažymėjimo išdavimo data ir galiojimo data		
29.	Gimimo data (metai, mėnuo, diena)	2.	
30.	Vardas, pavardė		
31.	Neįgaliojo pažymėjimo išdavimo data ir galiojimo data		

32.	Gimimo data (metai, mėnuo, diena)	3.
33.	Vardas, pavardė	
34.	Neįgaliojo pažymėjimo išdavimo data ir galiojimo data	
V. Kita		

_____ _____ _____

(darbuotojo vardas, pavardė) (parašas) (data)

Šiaulių technologijų mokymo centro
Asmens duomenų tvarkymo taisyklių
3 priedas

KANDIDATO SUTIKIMAS DĖL ASMENS DUOMENŲ TVARKYMO

_____
(*pildymo data, vieta*)

Aš, _____,
(kandidato vardas ir pavardė)

1. <u>Sutinku</u>/ <u>Nesutinku</u> (*nereikalingą išbraukti*), kad:

Šiaulių technologijų mokymo centras, darbuotojų atrankos vykdymo tikslu, tvarkytų šiuos mano asmens duomenis:

Vardas, pavardė	
Telefono numeris	
Išsilavinimas	
Užsienio kalbos	
Norimos pareigos	
Darbo patirtis	
Papildoma informacija	

2. **Patvirtinu**, kad mano pateikti duomenys yra teisingi, tikslūs ir išsamūs.

3. Centras visų kandidatų duomenis, dalyvaujančių atrankoje dėl darbo Centre, tvarkys šiuo tikslu:

3.1. naujo darbuotojo atrankos organizavimas;

3.2. kaštų optimizavimas.

4. Kandidatų CV ir kituose dokumentuose pateikti asmens duomenys bus tvarkomi darbuotojų atrankos proceso metu. Atrankos pabaiga laikoma darbo sutartį pasirašiusio kandidato išbandymo laikotarpio (t.y. daugiausiai 3 mėnesiai) pasibaigimo diena. Atrankos procesui pasibaigus, neatrinktų kandidatų pateikti duomenys (įskaitant CV) bus nedelsiant sunaikinami nebent Jūs patys nurodytumėte kitaip.

5. Teisiniai kandidatų duomenų tvarkymo pagrindai:

5.1. teisėti Centro interesai (darbuotojų įdarbinimas, laiko sąnaudų bei finansinių išteklių darbuotojų paieškai optimizavimas);

5.2. sutikimas dėl duomenų tvarkymo pasibaigus šiai atrankai.

6. **Man yra žinoma**, kad aš turiu teisę:

6.1. būti informuotas apie savo asmens duomenų tvarkymą;

6.2. susipažinti su tvarkomais mano asmens duomenimis ir žinoti, kaip jie yra tvarkomi;

6.3. reikalauti ištaisyti neteisingus, neišsamius, netikslius savo asmens duomenis;

6.4. nesutikti (pareiškiant nesutikimą raštu), kad būtų tvarkomi mano asmens duomenys.

7. Esu informuotas, kad turiu teisę atšaukti šį savo duotą sutikimą bet kuriuo metu, informuodamas apie tai Centrą raštu.

8. Man yra žinomos kitos mano, kaip duomenų subjekto, teisės, nustatytos 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB ir kituose asmens duomenų apsaugą reglamentuojančiuose teisės aktuose.

9. Patvirtinu, kad Centras mane tinkamai ir visapusiškai supažindino su šio Sutikimo davimo tikslu, galimomis pasekmėmis, mano teisėmis.

10. Patvirtiname, kad duomenis tvarkome laikydamiesi galiojančių Europos Sąjungos bei Lietuvos Respublikos teisės aktų reikalavimų bei kontroliuojančių institucijų nurodymų. Centre taikomos visos protingos techninės ir administracinės priemonės tam, kad mūsų surinkti duomenys būtų apsaugomi nuo praradimo, neleistino naudojimo ir pakeitimų. Mūsų darbuotojai yra raštiškai įsipareigoję trečiosioms šalims neatskleisti ir neplatinti darbo vietoje gaunamos informacijos įskaitant ir informacijos apie kandidatus į darbo vietas. Jūsų duomenys nėra perduodami kitiems gavėjams. Jeigu nurodysite kontaktinius asmenis, kurie galėtų Jus rekomenduoti, prašome juos informuoti apie tai, kad perdavėte jų kontaktus mums ir mes galime su jais artimiausiu metu susisiekti. Be Jūsų sutikimo nesusisieksime su Jūsų esamu darbdaviu, su buvusiais darbdaviais galime susisiekti apie tai pranešdami atskirai.

Sutikimas dėl tolimesnio kandidato duomenų saugojimo.

Jeigu pageidaujate, kad Centras saugotų Jūsų CV ir kitus įdarbinimo metu surinktus duomenis dar 1 metus ateities darbo pasiūlymams, pažymėkite (pabraukdami tinkamą variantą) apie šį savo pageidavimą žemiau. Informuojame, kad Jūs turite teisę nesutikti, o sutikę - bet kada atšaukti šį savo sutikimą. Jūsų atsakymas neturės jokios neigiamos įtakos nei šiame įdarbinimo procese, nei ateityje.

Sutinku/Nesutinku, kad Centras saugotų mano CV ateities darbo pasiūlymams, kaip tai nurodyta aukščiau.

_____	_____	_____
Vardas, pavardė	Parašas	Data

Šiaulių technologijų mokymo centro
Asmens duomenų tvarkymo taisyklių
4 priedas

(Pranešimo apie asmens duomenų saugumo pažeidimą forma Centro viduje)

Šiaulių technologijų mokymo centras

_____
(struktūrinio padalinio pavadinimas)

_____
(pareigų pavadinimas)

_____
(vardas, pavardė)

PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____ Nr. _____
(data, dokumento numeris)

_____
(vieta)

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

2. Asmens duomenų saugumo pažeidimo esmė ir aplinkybės:
_____
_____

3. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (pvz., Centro darbuotojai, mokiniai kt.) ir apytikslis jų skaičius:
_____
_____

4. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-us):
☐ Darbuotojų asmens tapatybę patvirtinantys duomenys (vardas, pavardė, gimimo data ir kt.)
☐ Mokinių asmens tapatybę patvirtinantys duomenys (vardas, pavardė, gimimo data ir kt.)
☐ Asmens kontaktiniai duomenys (gyvenamosios vietos adresas, tel. numeris, el. pašto adresas ir kt.)
☐ Specialių kategorijų asmens duomenys (duomenys, susiję su asmens sveikata, genetiniai duomenys ir kt.)
☐ Kiti asmens duomenys (įrašyti):
_____
_____

5. 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)

Šiaulių technologijų mokymo centro
Asmens duomenų tvarkymo taisyklių
5 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
☐ 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.):
_____

☐ Kiti asmens duomenys:

_____

1.5. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius:_____
1.6. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (Centro darbuotojai, mokiniai ir kt.):

_____

1.7. Apytikslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius:_____
1.8. Darbuotojas, pranešęs apie asmens duomenų saugumo pažeidimą (vardas, pavardė, Centro 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)

_____

Šiaulių technologijų mokymo centro
Asmens duomenų tvarkymo taisyklių
6 priedas

(Pranešimo apie asmens duomenų saugumo pažeidimą forma)

(duomenų valdytojo (juridinio asmens) pavadinimas, duomenų valdytojo atstovo pavadinimas, duomenų valdytojo (fizinio asmens) vardas, pavardė)[1]

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

(telefono ryšio numeris 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):
□ Informacinė sistema
□ Duomenų bazė
□ Tarnybinė stotis
□ Internetinė svetainė
□ Debesų kompiuterijos paslaugos
□ Nešiojami / mobilus įrenginiai
□ Neautomatiniu būdu susistemintos bylos (archyvas)
□ Kita _____

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)

[1] Kai pranešimas apie asmens duomenų saugumo pažeidimą teikiamas pagal Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymo (toliau – Įstatymas) 29 straipsnį, nurodomi tik duomenų valdytojo (juridinio asmens) duomenys.

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

_____

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.):

_____

_____

□ 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):

_____

_____

□ Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:

_____

_____

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

_____

_____

□ Kiti:

_____

_____

□ Nežinomi (pranešimo teikimo metu)

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

_____

1.8. Išsamiau apibūdinkite asmens duomenų saugumo pažeidimą, nurodykite (jei žinote) priežastis dėl kurių įvyko asmens duomenų saugumo pažeidimas ir pateikite kitą, duomenų valdytojo nuomone, reikšmingą informaciją:

_____

_____

_____

_____

1.9. Pranešimas kitoms įstaigoms pagal kompetenciją:

□ Ar informacija apie šį pažeidimą buvo perduota Lietuvos policijai? (jei galimai pažeidimas turi nusikalstamos veikos požymių)

□ Ar informacija apie šį pažeidimą buvo perduota Nacionaliniam kibernetinio saugumo centrui? (jei galimai pažeidimas galėjo paveikti kibernetinio saugumo subjektų ryšių ir informacines sistemas)

2. Galimos asmens duomenų saugumo pažeidimo pasekmės

2.1. Konfidencialumo praradimo atveju:
□ 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
_____
_____
_____
_____

2.2. Vientisumo praradimo atveju:
□ 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
_____
_____
_____
_____
_____

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
_____
_____
_____
_____
_____

2.4. Kita:
_____
_____
_____
_____

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

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:

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

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

□ 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)

_____
_____

□ Ne, nes dar neidentifikuoti duomenų subjektai, kurių asmens duomenų saugumas pažeistas

_____
_____
_____

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

_____

_____

5.4. Būdas, kokiu duomenų subjektai buvo informuoti:

□ Paštu

□ Elektroniniu paštu

□ Kitu būdu _____

5.5. Informuotų duomenų subjektų skaičius _____

6. Asmuo galintis suteikti daugiau informacijos apie asmens duomenų saugumo pažeidimą (duomenų apsaugos pareigūnas ar kitas kontaktinis asmuo)[2]

6.1. Vardas ir pavardė _____

6.2. Telefono ryšio numeris _____

6.3. Elektroninio pašto adresas _____

6.4. Pareigos _____

6.5. Darbovietės pavadinimas ir adresas _____

7. Pranešimo pateikimo Valstybinei duomenų apsaugos inspekcijai pateikimo vėlavimo priežastys

_____

_____

_____

_____

8. Kita reikšminga informacija

_____

_____

_____

_____

_____ _____ _____

(pareigos) (parašas) (vardas, pavardė)

_____

[2] Kai pranešimas apie asmens duomenų saugumo pažeidimą teikiamas pagal Įstatymo 29 straipsnį, nenurodomi šios formos 6.4 ir 6.5 papunkčiuose nurodyti duomenys.

Šiaulių technologijų mokymo centro
Asmens duomenų tvarkymo taisyklių
7 priedas

(Poveikio duomenų apsaugai vertinimo ataskaitos forma)

POVEIKIO DUOMENŲ APSAUGAI VERTINIMO ATASKAITA

_____

(*data*)

1. Priežastys, dėl kurių būtina atlikti poveikio duomenų apsaugai vertinimą

Planuojamos vykdyti veiklos aprašymas, jos tikslai ir planuojamos atlikti asmens duomenų tvarkymo operacijos. Paaiškinimas, kodėl būtina atlikti poveikio duomenų apsaugai vertinimą. Jei reikia, prie formos pridedami susiję dokumentai.

2. Asmens duomenų tvarkymo aprašymas

Aprašomi asmens duomenų rinkimo, naudojimo, saugojimo ir naikinimo veiksmai, nurodoma, iš kokių šaltinių bus renkami duomenys, kam bus teikiami (galima pateikti asmens duomenų tvarkymo veiksmų schemą). Aprašoma, kokie asmens duomenų tvarkymo veiksmai gali kelti pavojų fizinių asmenų teisėms ir laisvėms.

Aprašomas tvarkymo mastas: kokių kategorijų asmens duomenys bus tvarkomi; ar bus tvarkomi specialių kategorijų asmens duomenys arba duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas; kiek duomenų, kaip dažnai bus renkama ir naudojama; kaip ilgai bus saugomi asmens duomenys; nurodomas apytikslis duomenų subjektų skaičius bei geografinė duomenų tvarkymo aprėptis.

Aprašomas duomenų tvarkymo pobūdis: kokio pobūdžio santykiai sieja Jūsų Centrą su duomenų subjektais; ar duomenų subjektai turės galimybę kontroliuoti duomenų tvarkymą; ar duomenų subjektai gali numatyti, kad jų asmens duomenys bus tvarkomi šiuo būdu; ar bus tvarkomi vaikų ir kitų pažeidžiamų asmenų duomenys; įvertinama, ar toks duomenų tvarkymas yra saugus; ar duomenų tvarkymo technologijos yra naujos, ar egzistuojančios technologijos bus panaudotos kitokiu būdu; koks yra technologijų išsivystymo lygis šioje srityje; ar yra kokių nors visuomeninių ar pan. problemų ar klausimų, į kuriuos būtina atsižvelgti; nurodoma, ar yra įsipareigojimas laikytis patvirtinto elgesio kodekso ar patvirtinto sertifikavimo mechanizmo.

Aprašomi asmens duomenų tvarkymo tikslai: kokį rezultatą siekiama gauti; kokį poveikį tai turės fiziniams asmenims; kokia yra tokio duomenų tvarkymo nauda Jūsų Centrui bei kitiems asmenims.

3. Būtinumo ir proporcingumo įvertinimas

Aprašomas asmens duomenų tvarkymo teisėtumas ir tvarkymo proporcingumas: nurodomas teisėto tvarkymo pagrindas; įvertinama, ar tvarkant asmens duomenis bus pasiektas Jūsų tikslas; ar tą patį rezultatą įmanoma pasiekti kitokiu būdu; kokiu būdu bus išvengta veiklos sutrikimų; kaip bus užtikrinta duomenų kokybė ir įgyvendintas duomenų kiekio mažinimo principas; kokia informacija bus pateikta duomenų subjektams; kaip Jūsų Centras planuoja įgyvendinti duomenų subjektų teises; kokiu būdu bus užtikrinta, kad duomenų tvarkytojas laikytųsi reikalavimų; kokiu būdu bus užtikrintas į užsienio valstybes teikiamų asmens duomenų saugumas.

4. Kriterijų, rodančių galimą didelį pavojų duomenų subjektų teisės ir laisvėms, vertinimas:

Eil. Nr.	**Kriterijus**	**Egzistuoja/neegzistuoja**
1.	Naudojamas asmens duomenų ar duomenų subjektų vertinimas ir balų skyrimas, įskaitant profiliavimą ir prognozavimą	
2.	Automatizuotas sprendimų, sukeliančių teisinį arba panašų rimtą poveikį, priėmimas	
3.	Sisteminga asmens duomenų ar duomenų subjektų stebėsena	
4.	Neskelbtini duomenys arba labai asmeniški duomenys, pvz., specialių kategorijų asmens duomenys	
5.	Didelio masto duomenų tvarkymas	
6.	Duomenų rinkinių siejimas ir derinimas	
7.	Su pažeidžiamais duomenų subjektais susiję duomenys, pvz., vaikų duomenys, darbuotojai, pažeidžiamesni subjektai, kuriems reikalinga speciali apsauga, segmentai, kai galima nustatyti nelygiaverčius duomenų subjekto ir duomenų valdytojo santykius	
8.	Naujų technologijų ar organizacinių sprendimų būdų taikymas	
9.	Dėl duomenų tvarkymo duomenų subjektams užkertamas kelias naudotis savo teisėmis, paslaugomis arba sudaryti sutartis	
10.	Kitos aplinkybės, rodančios galimą didelį pavojų subjektų teisėms ir laisvėms	

5. Pavojų nustatymas ir įvertinimas

Aprašomas pavojaus ir poveikio fiziniam asmeniui pobūdis. Jei būtina, aprašoma susijusi verslo rizika.	**Žalos tikimybė**	**Žalos sunkumas**	**Bendras pavojaus lygis**
	Mažai tikėtina, tikėtina ar labai tikėtina	Minimali, reikšminga ar sunki	Žemas, vidutinis ar aukštas

6. Duomenų tvarkymo operacijos atitikties Reglamento ir kitų teisės aktų, reglamentuojančių asmens duomenų apsaugą, vertinimas:

7. Pavojams, grėsmėms duomenų subjektų teisėms ir laisvėms (V dalis) bei galimam neatitikimui Reglamentui ir kitiems teisės aktams, reglamentuojantiems asmens duomenų apsaugą (VI dalis), pašalinti numatytos priemonės, įskaitant apsaugos priemones, saugumo priemones ir mechanizmus, kuriais užtikrinama asmens duomenų apsauga ir pagrindžiama, kad bus laikomasi Reglamento ir kitų teisės aktų, reglamentuojančių asmens duomenų apsaugą:

Nurodomos papildomos priemonės, kurių galima imtis siekiant sumažinti ar panaikinti aukšto ar vidutinio lygio pavojus.

Pavojus	Priemonės sumažinti ar pašalinti pavojų	Priemonės pritaikymo rezultatas	Likęs pavojus	Priemonė patvirtinta
		Pašalinta, sumažinta, priimtina rizika	Žemas, vidutinis ar aukštas	Taip, ne

8. Išvados ir sprendimai

Nurodomos priemonės ir įvardijamas likęs pavojus	Atsakingas subjektas/padalinys
Priemonės patvirtintos:	
Likęs pavojus pripažintas priimtina rizika: *Jei priimtina rizika pripažintas aukšto lygio pavojus priimtinas, privaloma kreiptis dėl išankstinės konsultacijos į Valstybinę duomenų apsaugos inspekciją*	

9. Duomenų subjektų ar jų atstovų nuomonė apie numatomą duomenų tvarkymą, jeigu tokia nuomonė yra gauta, argumentai ir motyvai, jeigu nusprendžiama neatsižvelgti į duomenų subjektų ar jų atstovų nuomonę, arba priežastys, dėl kurių nesiekiama išsiaiškinti duomenų subjektų ar jų atstovų nuomonės:

Nurodomos ir glaustai aprašomos kitų asmenų nuomonės ir nurodoma, ar į jas atsižvelgta. Jeigu sprendimas skiriasi nuo susijusių asmenų nuomonės, pagrindžiama, kodėl.

10. Duomenų apsaugos pareigūno nuomonė ir konsultacijos dėl poveikio duomenų apsaugai vertinimo:

Duomenų apsaugos pareigūno nuomonė turi būti pateikta dėl asmens duomenų tvarkymo teisėtumo, planuojamų priemonių pavojams mažinti ar pašalinti bei dėl galimybės toliau tvarkyti asmens duomenis.

Nurodoma duomenų apsaugos pareigūno nuomonė ir konsultacijos dėl poveikio duomenų apsaugai vertinimo:

11. Nurodoma, ar atsižvelgta į duomenų apsaugos pareigūno nuomonę

Jeigu atmesta, pagrindžiama, kodėl.

12. Pasitelktų konsultantų, specialistų, ekspertų nuomonė ir išvados (*jeigu konsultantai, specialistai, ekspertai buvo pasitelkti*):

Nurodoma Pasitelktų konsultantų, specialistų, ekspertų nuomonė ir išvados:

13. Poveikio duomenų apsaugai vertinimo išvados (ar duomenų tvarkymo operacijos kelia riziką dėl didelio pavojaus duomenų subjektų teisėms ir laisvėms ar neatitikties Reglamento ar kitų teisės aktų nuostatoms, ar numatytos priemonės (VII dalis) sumažina riziką iki priimtino lygio, ar yra pagrindas konsultuotis su Valstybine duomenų apsaugos inspekcija):

14. Poveikio duomenų apsaugai vertinimą atlikę asmenys, jų parašai:

_____

(vardas, pavardė, pareigos, parašas)

_____

(vardas, pavardė, pareigos, parašas)

15. Už šio poveikio duomenų apsaugai vertinimo priežiūrą paskirtas atsakingas asmuo

Pastaba. *Duomenų apsaugos pareigūnas turi prižiūrėti asmens duomenų tvarkymo atitiktį Poveikio duomenų apsaugai vertinime nurodytoms išvadoms ir sprendimams.*

_____

(vardas, pavardė, pareigos, parašas)

Šiaulių technologijų mokymo centro
Asmens duomenų tvarkymo taisyklių
8 priedas

„PRIVACY BY DEFAULT“ IR „PRIVACY BE DESIGN“ DUOMENŲ APSAUGOS PRINCIPŲ TAIKYMO GAIRĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Šiaulių technologijų mokymo centro (toliau – Centras) pritaikytosios duomenų apsaugos (angl. privacy by default) ir standartizuotos duomenų apsaugos (angl. privacy by design) principų gairės (toliau – Gairės) nustato pritaikytosios ir standartizuotos duomenų apsaugos principų taikymo Centre tvarką.

2. Gairės parengtos vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Reglamentas) bei kitais teisės aktais, reglamentuojančiais asmens duomenų tvarkymą.

3. Gairėmis privalo vadovautis visi Centro darbuotojai.

4. Visos Centre vykdomos asmens duomenų tvarkymo operacijos, kurios gali kelti riziką asmenų privatumui, turi būti iš anksto papildomai įvertinamos ir valdomos.

5. Reglamentas reikalauja, kad duomenų valdytojai asmens privatumo klausimus apsvarstytų visų projektų pradinėse stadijose ir atitinkamai pakoreguotų tvarkomų asmens duomenų kiekį, tikslus ir saugumo priemones – šis procesas vadinamas Pritaikytoji duomenų apsauga.

6. Asmenų privatumas turi būti užtikrinamas ne vien tik teisinėmis, bet ir techninėmis priemonėmis, todėl pritaikytos duomenų apsaugos principas reikalauja, kad būtų įvertinama galima rizika ir nustatomos techninės priemonės, kurios padės tą riziką suvaldyti.

II SKYRIUS
STANDARTIZUOTA DUOMENŲ APSAUGA

7. Standartizuota duomenų apsauga reiškia, kad Centre visose srityse turi būti tvarkomi tik tie asmens duomenys, kurie yra griežtai būtini konkrečiam tikslui pasiekti.

8. Standartizuota duomenų apsauga reiškia, kad Centre veikiančios IT technologijos, sistemos ir aplikacijos turi turėti tokius automatinius nustatymus (*angl. default settings),* kurie leistų jomis naudotis be asmens duomenų pateikimo.

9. Ten kur, naudojantis Centre veikiančiomis IT technologijomis, sistemomis ir aplikacijomis, reikalinga identifikacija, užtikrinti, kad būtų naudojamas automatinis asmens duomenų šifravimas.

10. Elektroninėje erdvėje, standartizuotas duomenų apsaugos principas reiškia, kad teikiamų elektroninių paslaugų standartiniai nustatymai (*angl. default privacy settings*), turi būti patys griežčiausi, tai yra, kad būtų renkama tik tiek asmens duomenų, kiek reikia nustatytam tikslui pasiekti.

11. Standartinės Centro pasirinktos techninės ir organizacinės priemonės turi apimti:

11.1. kuo mažesnės apimties asmens duomenų tvarkymą;

11.2. kuo skubesnį pseudonimų suteikimą asmens duomenims;

11.3. asmens duomenų tvarkymo skaidrumą;

11.4. nuolatinį duomenų apsaugos priemonių Centre kūrimą ir tobulinimą.

III SKYRIUS
PRITAIKYTOJI DUOMENŲ APSAUGA

12. Pritaikytoji duomenų apsauga yra proaktyvi veikla, reiškianti, kad Centras turi imtis aktyvių veiksmų asmens duomenų saugumui užtikrinti. Tokie aktyvūs veiksmai yra bendri Centro

darbuotojų susitikimai, technologinių sprendimų diegimas, Poveikio duomenų apsaugai atlikimas, domėjimasis technologinėmis naujovėmis, kurios padeda užtikrinti duomenų saugumą, darbuotojų švietimas ir pan.

13. Pritaikytoji duomenų apsauga yra prevencinė, o ne taisomoji veikla, kas reiškia, kad prieš pradedant duomenų rinkimą, turi būti svarstomas jų tvarkymo poreikis. Pritaikytoji duomenų apsauga reiškia, kad apie asmens duomenų tvarkymą ir saugumą Centre turi būti galvojama ne po to, kai jau yra gauti asmens duomenys, bet iki pradedant juos tvarkyti.

14. Pritaikyta duomenų apsauga reiškia, kad Centras, planuodamas nauju būdu tvarkyti asmens duomenis, į duomenų apsaugą turi atsižvelgti pradiniuose tokio planavimo etapuose, įtraukiant atsakingus asmenis iš IT ir teisinės srities.

15. Pritaikytoji duomenų apsauga reiškia, kad Centro IT sistemos turi būti sukurtos taip, kad leistų įgyvendinti visas duomenų subjektų teises, įskaitant teisę būti pamirštam.

16. Pritaikytoji duomenų apsauga reiškia, kad kuriant naują platformą, aplikaciją, puslapį ar kitą elektroninį įrankį, turi būti svarstoma, ar jam įgyvendinti bus reikalingi asmens duomenys ir ar galima būtų apsieiti be asmens duomenų tvarkymo.

17. Pritaikytoji duomenų apsauga reiškia, kad Centre asmens duomenų tvarkymo saugumas turi būti užtikrinamas visą duomenų tvarkymo Centre ciklą, nuo jų gavimo iki sunaikinimo.

18. Pasitelkiant naujus duomenų tvarkytojus Centre, turi atsakingai vertinti tvarkytojų turimas technines saugumo priemones ir nustatyti, ar jos leis įgyvendinti duomenų subjektų teises, ypač teisę būti pamirštam.

19. Centras turi peržiūrėti savo sutartis su duomenų tvarkytojais ir nuolatos vertinti, ar tvarkytojams perduodama tik tiek asmens duomenų, kiek reikia jų funkcijoms atlikti.

20. Už tam tikrą projektą atsakingas asmuo, planuodamas nauju būdu tvarkyti asmens duomenis, arba esamas duomenų tvarkymo operacijas papildyti naujais asmens duomenimis, privalo informuoti Centro duomenų apsaugos pareigūną ir įtraukti jį į visas projektavimo stadijas.

21. Duomenų apsaugos pareigūnas, nusprendžia, ar planuojama veikla, gali turėti neigiamų pasekmių asmenų privačiam gyvenimui ir ar reikia atlikti Poveikio duomenų apsaugai vertinimą. Ši procedūra numatyta Centro Asmens duomenų tvarkymo taisyklėse „Poveikio duomenų apsaugai vertinimas“.

IV SKYRIUS
BAIGIAMOSIOS NUOSTATOS

22. Gairės gali būti keičiamos ir (ar) papildomos, atsižvelgiant į pasikeitusias teisės aktų, reglamentuojančių asmens duomenų tvarkymą, nuostatas, technologinius pokyčius ir Centro poreikius.

23. Centro darbuotojai ir kiti atsakingi asmenys su Gairėmis supažindinami pasirašytinai arba elektroninėmis priemonėmis ir, atlikdami savo darbo funkcijas, privalo vadovautis Gairėse nustatytais principais bei tvarka. Priėmus naują vadovaujančių pareigų darbuotoją, jis su Gairėmis privalo būti supažindintas pirmąją jo darbo dieną.

Šiaulių technologijų mokymo centro
Asmens duomenų tvarkymo taisyklių
9 priedas

Duomenų valdytojo duomenų tvarkymo veiklos įrašas

<table>
<tr><td colspan="4">Duomenų valdytojas:</td></tr>
<tr><td colspan="4">Duomenų valdytojo (jei taikoma, ir bendro duomenų valdytojo) ar jo atstovo pavadinimas (jei fizinis asmuo – vardas ir pavardė)</td></tr>
<tr><td>Pašto adresas</td><td>Telefono ryšio numeris</td><td>Elektroninio pašto adresas</td><td>Kitos ryšių priemonės (pvz., el. siuntos pristatymo dėžutės adresas ar kt.)</td></tr>
<tr><td colspan="4">Duomenų apsaugos pareigūnas:</td></tr>
<tr><td colspan="4">Duomenų apsaugos pareigūno vardas ir pavardė</td></tr>
<tr><td>Pašto adresas</td><td>Telefono ryšio numeris</td><td>Elektroninio pašto adresas</td><td>Kitos ryšių priemonės</td></tr>
<tr><td colspan="4">Duomenų tvarkymo tikslas (pvz., asmenų atrankos į laisvas pareigas organizavimas ir administravimas; vykdomųjų raštų vykdymas ir administravimas; prekių ir (ar) paslaugų pardavimas; tiesioginė rinkodara; interneto svetainės lankomumo vertinimas; turto saugumo užtikrinimas (kai vykdomas vaizdo stebėjimas), paslaugų kokybės užtikrinimas (kai vykdomas telefoninių pokalbių įrašymas; automobilio nuomos sutarčių sudarymo, vykdymo, apskaitos ir t. t.).</td></tr>
<tr><td colspan="4">Duomenų subjektų kategorijų aprašymas (pvz., darbuotojai; asmenys, patenkantys į vaizdo stebėjimo lauką; pirkėjai, klientai; interneto svetainės lankytojai; mokiniai; pacientų įgalioti atstovai ir t. t.)</td></tr>
<tr><td colspan="4">Asmens duomenų kategorijų aprašymas (pvz., vardas, pavardė, gimimo data, gyvenamosios vietos adresas, atvaizdas, darbo užmokestis, duomenys apie sveikatą, telefono ryšio numeris, telefono pokalbio įrašas, IP adresas, parašas ir t. t.) Esant kelioms duomenų subjektų grupėms, atskirai nurodomi tvarkomi asmens duomenys apie kiekvieną duomenų subjektų grupę (įskaitant ir specialių kategorijų asmens duomenis), jeigu tvarkomi asmens duomenys yra skirtingi.</td></tr>
<tr><td colspan="4">Duomenų gavėjų kategorijos (duomenų gavėjai, kuriems buvo arba bus atskleisti ar kitaip perduoti asmens duomenys, įskaitant duomenų gavėjus trečiosiose valstybėse ar tarptautines organizacijas) (pvz., draudimo bendrovės, kurjerių tarnybos, duomenų tvarkytojai, bankai ir t. t.)</td></tr>
<tr><td colspan="4">Asmens duomenų perdavimas į trečiąją valstybę arba tarptautinei organizacijai (kai taikoma):</td></tr>
<tr><td colspan="2">Trečiosios valstybės arba tarptautinės organizacijos, kuriai perduodami asmens duomenys pavadinimas:</td><td colspan="2">BDAR 49 straipsnio 1 dalies antroje pastraipoje nurodytais duomenų perdavimų atvejais tinkamų apsaugos priemonių dokumentai:</td></tr>
<tr><td colspan="4">Kita informacija, susijusi su asmens duomenų perdavimu:</td></tr>
<tr><td colspan="4">Numatomi asmens duomenų saugojimo, ištrynimo terminai (kai įmanoma) (pvz., 10 metų po sutarties įvykdymo, 72 valandos nuo prašymo gavimo, 1 metai nuo paskutinio prisijungimo prie kliento paskyros ir t. t.)</td></tr>
<tr><td colspan="4">Bendras duomenų saugumo priemonių (nurodytų BDAR 32 straipsnio 1 dalyje) aprašymas (kai įmanoma):</td></tr>
<tr><td colspan="2">Techninės saugumo priemonės:
(pvz., programinė įranga yra nuolatos atnaujinama, aprūpinta ugniasienėmis ir antivirusinėmis programomis, daromos atsarginės duomenų kopijos, atliekamas duomenų šifravimas ir t. t.)</td><td colspan="2">Organizacinės saugumo priemonės:
(pvz., informacinių sistemų ir duomenų bazių vartotojų teisių ribojimas ir kontrolė, asmenys, dirbantys su asmens duomenimis, yra saistomi teisės aktuose nustatytų konfidencialumo pareigų ir t. t.)</td></tr>
<tr><td colspan="4">Kita informacija (pvz., duomenų šaltiniai, duomenų tvarkymo teisiniai pagrindai, darbuotojai (skyriai), atsakingi už duomenų tvarkymą, duomenų subjekto teisių įgyvendinimo ypatumai, nuorodos į kitus su duomenų apsauga susijusius dokumentus (į poveikio duomenų apsaugai vertinimą, vidaus tvarkos taisykles ir t. t.)</td></tr>
<tr><td colspan="4">Duomenų tvarkymo veiklos įrašų užpildymo, atnaujinimo data (-os)</td></tr>
</table>

Šiaulių technologijų mokymo centro
Asmens duomenų tvarkymo taisyklių
10 priedas

Duomenų tvarkytojo duomenų tvarkymo veiklos įrašas

Duomenų tvarkytojas:			
Duomenų tvarkytojo ar jo atstovo pavadinimas (jei fizinis asmuo – vardas ir pavardė)			
Pašto adresas	*Telefono ryšio numeris*	*Elektroninio pašto adresas*	*Kitos ryšių priemonės (pvz., el. siuntos pristatymo dėžutės adresas ar kt.)*
Kiekvienas duomenų valdytojas (jei taikoma – ir jo atstovas)**, kurio vardu veikia duomenų tvarkytojas:**			
Duomenų valdytojo pavadinimas (jei fizinis asmuo – jo vardas ir pavardė)			
Pašto adresas	*Telefono ryšio numeris*	*Elektroninio pašto adresas*	*Kitos ryšių priemonės*
Duomenų apsaugos pareigūnas (jei taikoma)**:**			
Duomenų apsaugos pareigūno vardas ir pavardė			
Pašto adresas	*Telefono ryšio numeris*	*Elektroninio pašto adresas*	*Kitos ryšių priemonės*
Kiekvieno duomenų valdytojo vardu atliekamo duomenų tvarkymo kategorijos, t. y. atliekami asmens duomenų tvarkymo veiksmai *(pvz., vaizdo stebėjimas, asmens duomenų saugojimas, naikinimas ir t. t.)*			
Asmens duomenų perdavimo į trečiąją valstybę arba tarptautinei organizacijai (kai taikoma)**:**			
Trečiosios valstybės arba tarptautinės organizacijos, kuriai perduodami asmens duomenys, pavadinimas:		BDAR 49 straipsnio 1 dalies antroje pastraipoje nurodytais duomenų perdavimų atvejais tinkamų apsaugos priemonių dokumentai:	
Kita informacija, susijusi su asmens duomenų perdavimu			
Bendras duomenų saugumo priemonių (nurodytų BDAR 32 straipsnio 1 dalyje) **aprašymas** (kai įmanoma)**:**			
Techninės saugumo priemonės: *(pvz., programinė įranga yra nuolatos atnaujinama, aprūpinta ugniasienėmis ir antivirusinėmis programomis, daromos atsarginės duomenų kopijos, atliekamas duomenų šifravimas ir t. t.)*		Organizacinės saugumo priemonės: *(pvz., informacinių sistemų ir duomenų bazių vartotojų teisių ribojimas ir kontrolė, asmenys, dirbantys su asmens duomenimis, yra saistomi teisės aktuose nustatytų konfidencialumo pareigų ir t. t.)*	
Kita informacija *(pvz., darbuotojai (skyriai), atsakingi už duomenų tvarkymą, nuorodos į kitus su duomenų apsauga susijusius dokumentus ir t. t.)*			
Duomenų tvarkymo veiklos įrašų užpildymo, atnaujinimo data (-os)			

Šiaulių technologijų mokymo centro
Asmens duomenų tvarkymo taisyklių
11 priedas

(Tvarkomų asmens duomenų inventorizacijos sąrašo forma)

TVARKOMŲ ASMENS DUOMENŲ INVENTORIZACIJOS SĄRAŠAS

Eil. Nr.	Asmens duomenų subjektų grupės[1]	Asmens duomenų kategorijos[2]	Asmens duomenų gavimo šaltiniai[3]	Asmens duomenų tvarkymo tikslas[4]	Asmens duomenų tvarkymo pagrindas[5]	Duomenų gavėjų kategorijos[6]	Asmens duomenų saugojimo, ištrynimo laikotarpis[7]	Saugos priemonės[8]
Data:								

[1]Mokiniai, darbuotojai, pretendentai į darbo ar praktikos vietas, projektų/konkursų/renginių dalyviai, kontrahentai, medicininės reabilitacijos gavėjai ir kt.
[2]Vardas, pavardė, asmens kodas, gimimo data, gyvenamosios vietos adresas, telefono numeris, el. pašto adresas, tėvų ar globėjų vardai, pavardės, kontaktinė informacija kt.
[3] Mokinių, jų tėvų ar globėjų; darbuotojų; kandidatų į darbą/praktiką; projektų/konkursų/renginių organizatorių ir kt.
[4] Mokymo proceso organizavimo; Centro darbuotojų darbo organizavimo; pretendentų į Centro darbuotojų/praktikantų pareigas kandidatūros įvertinimo, personalo valdymo tikslu ir kt.
[5]Sutikimas; teisės aktuose numatyta pareiga; sutartis; teisėti interesai ir kt.
[6]Valstybinėms institucijoms, atliekant joms priskirtas funkcijas; kitoms švietimo įstaigos, vykdant mokinių švietimą, konkursus, renginius ir kt.
[7]Asmens duomenys saugomi ne ilgiau, nei to reikalauja duomenų tvarkymo tikslai ir teisės aktai. Duomenų saugojimo laikas nurodomas dokumentacijos plane, *pvz.: 10 metų nuo darbo santykių pasibaigimo ir t.t.*
[8]Techninės priemonės, *pvz., ugniasienės, antivirusinė programinė įranga, prieigos kontrolė.* Organizacinės saugumo priemonės*: asmens duomenų tvarkymo politika, darbuotojų mokymas, konfidencialumo laikymasis ir kt.*

Šiaulių technologijų mokymo centro
Asmens duomenų tvarkymo taisyklių
12 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.											

_____