

MOLĖTŲ VAIKŲ SAVARANKIŠKO GYVENIMO NAMAI
(Kodas 190985787)

PATVIRTINTA
Molėtų vaikų savarankiško
gyvenimo namų direktoriaus
2020-03-26 įsakymu Nr. V-26

ASMENS DUOMENŲ TVARKYMO TAISYKLĖS

TURINYS

I. BENDROSIOS NUOSTATOS.....	3
II. PAGRINDINIAI ASMENS DUOMENŲ TVARKYMO PRINCIPAI.....	6
III. ASMENS DUOMENŲ TVARKYMO TEISINIAI PAGRINDAI.....	7
IV. ASMENS DUOMENŲ TVARKYMO TIKSLAI, SAUGOJIMO TERMINAI IR DUOMENŲ TEIKIMAS TRETIESIEMS ASMENIMS.....	8
V. DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI	9
VI. VAIZDO DUOMENŲ TVARKYMAS	11
VII. REIKALAVIMAI DARBUOTOJAMS, TVARKANTIEMS ASMENS DUOMENIS IR JŲ ATSAKOMYBĖ	13
VIII. TECHNINĖS IR ORGANIZACINĖS DUOMENŲ SAUGUMO PRIEMONĖS	14
IX. ASMENS DUOMENŲ TVARKYMOUI TAIKOMŲ PRIEMONIŲ SĄRAŠAS	18
X. ASMENS DUOMENŲ TVARKYTOJAI IR GAVĖJAI	20
XI. DUOMENŲ SUBJEKTŲ TEISĖS IR JŲ ĮGYVENDINIMO TVARKA	21
XII. POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS (PDAV) IR IŠANKSTINĖS KONSULTACIJOS SU PRIEŽIŪROS INSTITUCIJA	26
XIII. NEATITIKČIŲ, INCIDENTŲ IR KOREKCINIŲ VEIKSMŲ VALDYMAS	27
XIV. ASMENS DUOMENŲ APSAUGOS PAREIGŪNAS	29
XV. BAIGIAMOSIOS NUOSTATOS	30
1 priedas	
Molėtų vaikų savarankiško gyvenimo namų asmens duomenų tvarkymo registravimo žurnalas	31
2 priedas	
Prašymo įgyvendinti duomenų subjekto teisę (-es) rekomenduojama forma	32
3 priedas	
Neatitikčių registravimo žurnalas	34
4 priedas	
Poveikio duomenų apsaugai vertinimo forma	35

I. BENDROSIOS NUOSTATOS

1. Asmens duomenų tvarkymo taisyklių (toliau - Taisyklės) tikslas reglamentuoti asmenų, kurių duomenis tvarko Molėtų vaikų savarankiško gyvenimo namai (toliau - Įstaiga) asmens duomenų tvarkymo tikslus, nustatyti jų teisių įgyvendinimo tvarką, įtvirtinti organizacines ir technines duomenų apsaugos priemones, reguliuoti asmens duomenų tvarkytojo pasitelkimo atvejus bei užtikrinti Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (toliau - ADTAĮ), Bendrojo duomenų apsaugos reglamento (ES) 2016/679 (toliau - BDAR), kitų teisės aktų, reglamentuojančių asmens duomenų tvarkymą ir apsaugą, laikymąsi ir įgyvendinimą.

2. Pagrindinės taisyklėse vartojamos sąvokos:

Asmens duomenys - bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (**duomenų subjektas**) tiesiogiai arba netiesiogiai, visų pirma pagal identifikatorių, pavyzdžiui vardą ir pavardę, asmens kodą, buvimo vietos duomenis arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius. Pavyzdžiui: vaizdo įrašas, garso įrašas, pirkinių istorija, naršymo svetainėje statistika, lojalumo kortelės numeris ir pan.

Duomenų subjektas - fizinis asmuo, kurio asmens duomenis tvarko duomenų valdytojas ar duomenų tvarkytojas. Pavyzdžiui: darbuotojas, klientas, vartotojas, gyventojas ir pan.

Asmens duomenų tvarkymas (toliau - duomenų tvarkymas) - bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, pavyzdžiui rinkimas, įrašymas, rūšiavimas, kaupimas, klasifikavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimasis arba sunaikinimas.

Duomenų valdytojas - fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų valdymo tikslus ir priemones.

Duomenų valdytojas (toliau- Įstaiga) - Molėtų vaikų savarankiško gyvenimo namai, 190985787, Smilgų g. 4, Molėtai.

Duomenų tvarkytojas - fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis. Pavyzdžiui: personalo apskaitos sistemos tiekėjas, informacinių technologijų, serverio, interneto parduotuvės sistemos ar talpinimo paslaugos tiekėjas ir pan.

Duomenų gavėjas - fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuriai atskleidžiami asmens duomenys, nesvarbu, ar tai trečioji šalis, ar ne. Valdžios institucijos, kurios pagal valstybės narės teisės aktus gali gauti asmens duomenis vykdydamos konkretų tyrimą, nelaikomos duomenų gavėjais; tvarkydamos tuos duomenis tos valdžios institucijos laikosi taikomų duomenų tvarkymo tikslus atitinkančių duomenų apsaugos taisyklių.

Trečioji šalis - fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri nėra duomenų subjektas, duomenų valdytojas, duomenų tvarkytojas, arba asmenys, kuriems tiesioginiu duomenų valdytojo ar duomenų tvarkytojo įgaliojimu leidžiama tvarkyti asmens duomenis. Pavyzdžiui Įstaigos darbuotojai, partneriai, tiekėjai, nuomotojai, Valstybinė mokesčių inspekcija, bankai ir pan.

Specialiųjų kategorijų asmens duomenys - asmens duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, taip pat genetiniai duomenys, biometriniai duomenys, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenys (asmens duomenys, susiję su fizine ar psichine fizinio asmens sveikata, įskaitant duomenis apie sveikatos priežiūros paslaugos teikimą, atskleidžiantys informaciją apie to fizinio asmens sveikatos būklę) arba duomenys apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją.

Duomenų apsaugos pareigūnas (toliau - Pareigūnas) - Įstaigos vadovo paskirtas darbuotojas ar paslaugų teikėjas, atliekantis BDAR nustatytas duomenų apsaugos pareigūno funkcijas.

Duomenų subjekto sutikimas - bet koks laisva valia duotas konkretus ir nedviprasmiškas tinkamai informuoto duomenų subjekto valios išreiškimas pareiškimu arba vienareikšmiais veiksmais kuriais jis sutinka, kad būtų tvarkomi su juo susiję asmens duomenys.

Įgalioti tvarkyti asmens duomenis darbuotojai - duomenų valdytojo darbuotojai (t. y. asmenys tarp kurių ir duomenų valdytojo yra sudarytos darbo sutartys) ir / arba kiti fiziniai asmenys, kurie sutarčių ar kitu pagrindu turi teisę tvarkyti duomenų valdytojo tvarkomus asmens duomenis.

Vaizdo stebėjimas - vaizdo duomenų, susijusių su fiziniu asmeniu, tvarkymas naudojant automatizuotas vaizdo stebėjimo priemones (vaizdo ir fotokameras ar pan.), nepaisant to, ar šie duomenys yra išsaugomi laikmenoje.

Vaizdo įrašas - vaizdo stebėjimo kameromis užfiksuoti ir vaizdo duomenų įrašymo įrenginiuose išsaugoti vaizdo duomenys.

Prieiga prie vaizdo įrangos - fizinė prieiga ar prieiga elektroninio ryšio priemonėmis, suteikianti asmeniui galimybę keisti, šalinti ar atnaujinti techninės vaizdo įrangos komponentes ar programinę įrangą, nustatyti vaizdo įrangos veikimo parametrus.

Asmens duomenų įrašymo įrenginiai - įstaigoje esantys skaitmeniniai įrenginiai, skirti vaizdo duomenims įrašyti, saugoti, peržiūrėti ir kopijuoti.

Interneto svetainė - Įstaigos svetainė, paskelbta adresu www.moletuvaikai.lt, kurioje yra pristatomos paslaugos.

Profilavimas - bet kokios formos automatizuotas Asmens duomenų tvarkymas, kai Asmens duomenys naudojami siekiant įvertinti tam tikrus su fiziniu asmeniu susijusius asmeninius aspektus, visų pirma siekiant išanalizuoti ar numatyti aspektus, susijusius su to asmens darbo rezultatais, ekonomine situacija, sveikatos būkle, asmeniniais pomėgiais, interesais, patikimumu, elgesiu, buvimo vieta arba judėjimu.

Techninės ir organizacinės saugumo priemonės - tai priemonės, kuriomis siekiama apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo ar netyčinio praradimo, pakeitimo, neteisėto atskleidimo ar prieigos, ypač tais atvejais, kai tvarkymas susijęs su duomenų perdavimu tinkle, ir visos kitos neteisėtos tvarkymo formos.

Duomenų bazė - yra organizuotas (susistemintas, metodiškai sutvarkytas) duomenų rinkinys, kuriuo galima individualiai naudotis elektroniniu ar kitu būdu.

Neatitiktis - bet koks įvykis, turėjęs ar galintis turėti įtakos asmens duomenų saugumui.

Informacijos saugumo įvykis - nustatytas sistemos, tarnybos ar tinklo įvykis, rodantis, kad yra galima saugumo užtikrinimo spraga ar apsaugos priemonių trikdys arba anksčiau nenumatyta situacija, kuri gali būti svarbi saugumui.

Informacijos saugumo incidentas - vienas ar daugiau nepageidaujamų ir netikėtų informacijos saugumo įvykių, turinčių didelę tikimybę pakenkti veiklai ir keliančių grėsmę informacijos saugumui.

Korekcinis veiksmas - veiksmas, atliekamas siekiant pašalinti nustatytos neatitikties ar kitos nepageidaujamos situacijos priežastį.

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

Asmens duomenų tvarkymo registravimo žurnalas - Įstaigos įgalioto darbuotojo pildomas žurnalas, skirtas Įstaigoje pateiktų prašymų, susijusių su asmens duomenų tvarkymu registracijai ir administravimui. Duomenų subjektų prašymus dėl tvarkomų duomenų priima ir Įstaigos Asmens

duomenų tvarkymo registravimo žurnale (Taisyklių priedas Nr. 1) užregistruoja Pareigūnas arba Įstaigos vadovo įgaliotas asmuo.

Tvarkymo veiklos įrašas - Įstaigos nustatytos formos dokumentas, kuriame fiksuojama Įstaigos vykdomų duomenų tvarkymo veiklų tikslai, duomenų subjektai, duomenų gavėjai, duomenų ištrynimo terminai ir kita reikalaujama arba reikšminga informacija apie duomenų tvarkymo veiklas.

Priežiūros institucija - Valstybinė duomenų apsaugos inspekcija (toliau - VDAI)

3. Taisyklėse vartojamos sąvokos atitinka ADTAĮ ir BDAR vartojamas sąvokas. Taisyklių nuostatos negali plėsti ar susiaurinti ADTAĮ ir BDAR taikymo srities bei prieštarauti ADTAĮ ir BDAR nustatytiems asmens duomenų tvarkymo reikalavimams ir kitiems asmens duomenų tvarkymą reglamentuojantiems teisės aktams.

4. Taisyklės taikomos tvarkant fizinių asmenų duomenis tiek automatiniu būdu, tiek neautomatiniu būdu tvarkant asmens duomenų susistemintas rinkmenas: klientų sąrašus, kartotekas, bylas, sąvadus ir kita. Taisyklės taip pat nustato Įstaigos darbuotojų teises, pareigas ir atsakomybę tvarkant asmens duomenis.

5. Taisyklių, pagrindinių asmens duomenų tvarkymo principų, konfidencialumo ir saugumo reikalavimai, įtvirtinti ADTAĮ ir (ar) BDAR bei šiose Taisyklėse, privalomi visiems Įstaigoje pagal darbo sutartis dirbantiems darbuotojams (toliau - Darbuotojas), kurie yra įgalioti tvarkyti Įstaigoje esančius asmens duomenis arba eidami savo pareigas juos sužino, bei kitiems sutartiniais pagrindais paslaugas teikiantiems asmenims, kurie gali tvarkyti arba sužino asmens duomenis.

6. Duomenų valdytojas turi šias teises:

6.1. rengti ir priimti vidinius teisės aktus, reglamentuojančius duomenų tvarkymą;

6.2. spręsti dėl tvarkomų asmens duomenų teikimo;

6.3. paskirti už asmens duomenų apsaugą atsakingus asmenis;

6.4. įgalioti duomenų tvarkytojus tvarkyti asmens duomenis.

7. Duomenų valdytojas turi šias pareigas:

7.1. užtikrinti ADTAĮ ir kituose teisės aktuose, reglamentuojančiuose asmens duomenų tvarkymą, nustatytų asmens duomenų tvarkymo reikalavimų laikymąsi;

7.2. įgyvendinti duomenų subjekto teises ADTAĮ ir šiose Taisyklėse nustatyta tvarka;

7.3. Užtikrinti asmens duomenų saugumą, įgyvendinant tinkamas organizacines ir technines asmens duomenų saugumo priemones;

7.4. parinkti tik tokius asmens duomenų tvarkymo įrangos priežiūros paslaugų tiekėjus, kurie garantuotų reikiamas technines ir organizacines asmens duomenų apsaugos priemones.

8. Duomenų valdytojas atlieka šias funkcijas:

8.1. nustato duomenų tvarkymo tikslą ir apimtį;

8.2. organizuoja duomenų tvarkymą;

8.3. analizuoja technologines, metodologines ir organizacines duomenų tvarkymo problemas ir priima sprendimus, reikalingus tinkamam duomenų tvarkymui užtikrinti;

8.4. teikia metodinę pagalbą darbuotojams duomenų tvarkymo klausimais;

8.5. organizuoja darbuotojų mokymus asmens duomenų teisinės apsaugos klausimais;

8.6. vykdo kitas funkcijas, reikalingas įgyvendinti asmens duomenų apsaugą.

II. PAGRINDINIAI ASMENS DUOMENŲ TVARKYMO PRINCIPAI

9. Įstaigoje asmens duomenys tvarkomi laikantis šių asmens duomenų tvarkymo ir apsaugos principų:

9.1. Asmens duomenis tvarkyti teisėtai, sąžiningai ir **skaidriai (teisėtumo, sąžiningumo ir skaidrumo principas)**;

9.2. Asmens duomenis rinkti nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkyti tikslais, nesuderinamai su nustatytaisiais prieš renkant asmens duomenis **(tikslų apibrėžimo principas)**; Tolesnis duomenų tvarkymas archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais nėra laikomas nesuderinamu su pirminiais tikslais. Įstaigos darbuotojai turi teisę rinkti, tvarkyti, perduoti, saugoti, naikinti ar kitaip naudoti asmens duomenis tik atlikdami savo tiesiogines funkcijas, apibrėžtas pareigybės aprašyme ar kitame Įstaigos lokaliniame nustatyta tvarka. Įstaigos darbuotojams draudžiama savavališkai rinkti, tvarkyti, perduoti, saugoti, naikinti ar kitaip naudoti asmens duomenis;

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

9.4. Tvarkomi asmens duomenys turi būti tikslūs ir prireikus atnaujinami; turi būti imamasi visų pagrįstų priemonių užtikrinti, kad asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba ištaisomi **(tikslumo principas)**;

9.5. Tvarkomus asmens duomenis laikyti tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi; asmens duomenis galima saugoti ilgesnius laikotarpius, jeigu asmens duomenys bus tvarkomi tik archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais, įgyvendinus atitinkamas technines ir organizacines priemones, kurių reikalaujama BDAR siekiant apsaugoti duomenų subjekto teises ir laisves **(saugojimo trukmės ribojimo principas)**;

9.6. Tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo **(vientisumo ir konfidencialumo principas)**;

9.7. Duomenų valdytojas yra atsakingas ir turi sugebėti įrodyti, kad yra laikomasi principų **(atskaitomybės principas)**.

10. Asmens duomenų tvarkymo principų laikymąsi užtikrina Įstaigos vadovas, imdamasis atitinkamų organizacinių priemonių (įsakymai, pavedimai ir pan.).

III. ASMENS DUOMENŲ TVARKYMO TEISINIAI PAGRINDAI

11. Įstaiga asmens duomenis tvarko tik esant bent vienam iš šių teisinių pagrindų:

11.1. Duomenų subjektas duoda sutikimą, kad jo asmens duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais.

11.2. Duomenų tvarkymas yra būtinas siekiant įvykdyti sutartį, kurios šalis yra duomenų subjektas, arba siekiant imtis veiksmų duomenų subjekto prašymu prieš sudarant sutartį;

11.3. Tvarkyti duomenis būtina, kad būtų įvykdyta duomenų valdytojui taikoma teisinė prievolė;

11.4. Tvarkyti duomenis būtina, siekiant apsaugoti duomenų subjekto ar kito asmens gyvybinius interesus (pavyzdžiui, Įstaiga tvarko darbuotojo artimųjų kontaktinius duomenis, su kuriais galėtų susisiekti įvykus nelaimei ar ekstremaliajam įvykiui);

11.5. Duomenų tvarkymas yra būtinas viešojo intereso labui arba vykdant pavestas viešosios valdžios funkcijas;

11.6. Tvarkyti duomenis būtina siekiant teisėtų duomenų valdytojo ar trečiosios šalies interesų, išskyrus atvejus, kai duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą, yra už šiuos duomenų valdytojo teisėtus interesus viršesni, ypač kai duomenų subjektas yra vaikas (pavyzdžiui, Įstaiga vykdo vaizdo stebėjimą darbuotojų, kitų duomenų subjektų ir turto saugumo užtikrinimo tikslu).

12. Įstaiga specialių kategorijų asmens duomenis tvarko tik esant bent vienam iš šių pagrindų:

12.1. Tvarkyti duomenis būtina, kad duomenų valdytojas arba duomenų subjektas galėtų įvykdyti prievolės ir naudotis specialiomis teisėmis darbo ir socialinės apsaugos teisės srityje, kiek tai leidžia Europos sąjungos arba valstybės narės teisėje arba pagal valstybės narės teisę sudaryta kolektyvine sutartimi, kuriuose nustatytos tinkamos duomenų subjekto pagrindinių teisių ir interesų apsaugos priemonės;

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

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 dėl viešojo intereso priežasčių visuomenės sveikatos srityje, siekiant apsaugoti nuo rimtų tarpvalstybinio pobūdžio grėsmių sveikatai.

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

13. Asmens duomenys Įstaigoje tvarkomi šiais tikslais (įskaitant, bet neapsiribojant atvejais kai gaunamas atskiras duomenų subjekto sutikimas dėl duomenų tvarkymo):

13.1. Vidaus administravimas: darbo sutarčių sudarymas, tinkamas vykdymas, apskaita (darbo užmokesčio ir kitų išmokų administravimas) ir nutraukimas; Praktikos sutarčių sudarymas; Mokymai; Duomenų valdytojo kaip darbdavio pareigų, nustatytų teisės aktuose, tinkamas vykdymas; Tinkamos komunikacijos su darbuotojais ne darbo metu palaikymas; Tinkamų darbo sąlygų užtikrinimas (struktūros tvarkymas, esamų ir buvusių darbuotojų informacijos valdymas, dokumentų valdymas, turimų materialinių ir finansinių išteklių valdymas);

13.2. Socialinės globos (rūpybos) teikimas vaikams nuo 0 iki 18 metų, o jei vaikas mokosi pagal bendrojo ugdymo programą, pagal formaliojo profesinio mokymo programą arba dalyvauja Jaunuolio savarankiško gyvenimo programoje - iki 21 metų; Globojamo (rūpinamo) ar laikinai globos namuose apgyvendinto vaiko globos (rūpybos), ugdymo, socialinių ilgalaikių bei trumpalaikių paslaugų, sudarant kitas jam tinkamas sąlygas ir palaikant aplinką, kurioje jis galėtų saugiai augti, vystytis ir tobulėti bei pasirengtų savarankiškam gyvenimui visuomenėje užtikrinimas; Kitiems asmenims, kuriems teikiama pagalba, ar asmenims dalyvaujantiems vykdomų projektų veikloje kompleksinės psichologinės, socialinės pagalbos teikimas, taip pat šių paslaugų administravimas. Pagalba į krizinę situaciją patekusiems asmenis ir šeimoms, globos centrui priklausantiems vaikams bei jų globėjams, tėvams. Asmens duomenų subjektai: tėvai, kurių vaikų, gaunančių trumpalaikės priežiūros ar dienos centro socialines paslaugas, amžius iki 16 m., ir kiti asmenys, kuriems teikiamos socialinės paslaugos sutikimą (kai asmens duomenys tvarkomi sutikimo pagrindu) dėl asmens duomenų tvarkymo išreiškia raštiškai, pagal nustatytą formą (Taisyklių 5, 6 priedas), patvirtindami, jog sutinka, kad jų asmens duomenys Įstaigoje būtų tvarkomi šiose Taisyklėse nurodytais tikslais. Duomenų subjektas turi teisę bet kuriuo metu atšaukti savo sutikimą, jeigu jo asmens duomenys tvarkomi neteisėtai. Sutikimo atšaukimas nedaro poveikio sutikimu pagrįsto duomenų tvarkymo, atlikto iki sutikimo atšaukimo, teisėtumui. Duomenų subjektas apie tai informuojamas prieš jam duodant sutikimą.

13.3. Gerųjų Įstaigos veiklos pavyzdžių, Įstaigos veiklos viešinimo, skelbiant asmens duomenis Įstaigos interneto svetainėje, pristatymuose ir kituose renginiuose ar medžiagoje visuomenės informavimo tikslais;

13.4. Įstaigos veiklos užtikrinimo tikslas (sutarčių sudarymo bei vykdymo, viešųjų pirkimų procedūrų organizavimas ir vykdymas, projektų rengimas ir vykdymas); Užklausų, komentarų ir nusiskundimų administravimas;

13.5. Teisių ir teisėtų interesų gynimas, siekiant apsaugoti Įstaigos darbuotojus nuo nepagrįstų mėginimų iškreipti jų žodžiu vykdomo pokalbio turinį (garso įrašymas per pasitarimus, susirinkimus, įdarbinimo konkursus);

13.6. Asmenų ir turto apsaugos tikslu vykdomas vaizdo stebėjimas (Vaizdo stebėjimo / filmavimo tvarkos aprašas).

14. Įstaiga tvarko asmens duomenis ne ilgiau negu būtina duomenų tvarkymo tikslams pasiekti.

15. Pasibaigus duomenų saugojimo terminui visi dokumentai, kuriuose yra asmens duomenų, visam laikui ištrinami, sunaikinami arba tampa anonimiais, t. y. neįmanoma nustatyti duomenų subjektų

tapatybės. Neištintus, nesunaikintus ar neanoniminius duomenis Įstaiga ištrins, sunaikins ar padarys anoniminiais rankiniu būdu iš karto po saugojimo termino pabaigos.

16. Už elektronine forma saugomų asmens duomenų rinkmenų sunaikinimą atsako konkrečiu kompiuteriu, kuriame saugomos asmens duomenų rinkmenos, dirbantis darbuotojas.

17. Už Įstaigos duomenų bazėse ir IT sistemose esančių duomenų sunaikinimą atsakingi šias sistemas administruojantys darbuotojai.

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

19. Kiekvienu tikslu atskirai, Įstaigoje sudaromas Tvarkymo veiklos įrašas, kuriame nurodomas duomenų saugojimo terminas, duomenų gavėjų kategorijos ir kita papildoma informacija.

V. DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI

20. Įstaiga privalo sudaryti ir tvarkyti duomenų Tvarkymo veiklos įrašus, kurie būtini tam, kad Įstaiga turėtų nuolatinę ir aktualią informaciją apie savo vykdomos duomenų tvarkymo veiklos apimtį, joje dalyvaujančius asmenis, naudojamas tvarkymo priemones.
21. Tvarkymo veiklos įrašų sudarymo formą ir formatą parengia Pareigūnas arba įgaliotas Įstaigos darbuotojas, atsižvelgdamas į Priežiūros institucijos rekomendacijas.
22. Tvarkymo veiklos įrašai yra Įstaigos vidaus dokumentai, kuriuose gali būti konfidencialios informacijos. Todėl Tvarkymo veiklos įrašai negali būti viešinami ir turi būti saugomi kaip kita Įstaigos konfidenciali informacija.
23. Siekiant užtikrinti Įstaigos atitiktis BDAR įrodymus, už Tvarkymo veiklos įrašų sudarymo, keitimo ir atnaujinimo organizavimą ir centralizuotą jų tvarkymą atsakingas Pareigūnas arba įgaliotas Įstaigos darbuotojas. Tačiau Įstaigos vadovas yra tiesiogiai atsakingas už informacijos, reikalingos Tvarkymo veiklos įrašams sudaryti, pakeisti ar atnaujinti, surinkimą, jų projektų paruošimą bei pateikimą Pareigūnui arba Įstaigos įgaliotam darbuotojui.
24. Kai Įstaigoje pradedamas ar keičiamas verslo procesas ar funkcija susiję su duomenų tvarkymu, Įstaigos vadovas turi užtikrinti, kad apie tokį procesą ar jų pokyčius būtų surinkta visa informacija, reikalinga Tvarkymo veiklos įrašui parengti ar pakeisti.
25. Duomenų Tvarkymo veiklos įrašai yra tvarkomi raštu. Rašytinei formai yra prilyginama ir elektroninė forma, saugoma kompiuteryje.
26. Tvarkant Tvarkymo veiklos įrašus turi būti užtikrinamas jų pakeitimų atsekamumas, tam kad būtų galima nustatyti, kokie pakeitimai buvo daromi Tvarkymo veiklos įrašuose, kada jie buvo atlikti ir dėl kokių priežasčių.
27. Tvarkymo veiklos įrašai turi būti pateikiami Priežiūros institucijai gavus jos prašymą. Už Tvarkymo veiklos įrašų pateikimą atsakingas Pareigūnas arba Įstaigos vadovo įgaliotas darbuotojas.

VI. VAIZDO DUOMENŲ TVARKYMAS

28. Įstaiga, siekdama užtikrinti darbuotojų, gyventojų, kitų duomenų subjektų saugumą, apsaugoti Įstaigos turtą nuo vagysčių ar sugadinimo tvarko duomenų subjektų vaizdo duomenis darydama vaizdo įrašus.

29. Vaizdo stebėjimas vykdomas adresu: **Smilgų g, 4, Molėtai.**

30. Duomenų subjektai apie vykdomą vaizdo stebėjimą informuojami informaciniais ženklais, įrengtais prieš duomenų subjektui patenkant į vaizdo stebėjimo lauką. Informaciniuose ženkluose pateikiama informacija apie tai, kad vykdomas vaizdo stebėjimas, nurodomas vaizdo stebėjimo tikslas, duomenų valdytojo pavadinimas, kontaktinė informacija (adresas, el. pašto adresas ir (arba) telefono ryšio numeris) ir nuoroda į interneto svetainę, kurioje galima rasti detalesnę informaciją apie asmens duomenų tvarkymą ir duomenų subjektų teisių įgyvendinimą.

31. Vaizdo duomenys vaizdo duomenų įrašymo įrenginiuose saugomi 15 parų, o nustačius pažeidimą - iki tyrimo pabaigos.

32. Vaizdo duomenis fiksuoja 7 vidaus ir 12 lauko vaizdo stebėjimo kamerų.

33. Duomenų subjektų interesai ir teisė į duomenų apsaugą ir privatumą nėra viršesni už Įstaigos interesus dėl šių priežasčių:

33.1. tvarkant asmens duomenis nėra tvarkoma informacija, susijusi su duomenų subjektų privačiu gyvenimu;

33.2. vaizdo stebėjimas Įstaigos patalpose vykdomas nedideliu mastu;

33.3. asmens duomenys nėra naudojami darbuotojų darbo kokybei vertinti;

33.4. nėra tvarkomi specialiųjų kategorijų asmens duomenys.

34. Įstaigos vadovo įgaliotas tvarkyti vaizdo duomenis darbuotojas privalo:

34.1. užtikrinti, kad į stebimą erdvę nepatektų gyvenamosios patalpos, įėjimai į jas, joms priklausančios teritorijos, patalpos, kuriose asmenys pagrįstai tikisi absoliučios privatumo apsaugos ir kur toks stebėjimas žemintų žmogaus orumą;

34.2. užtikrinti, kad vaizdo stebėjimo sistema būtų techniškai tvarkinga, techniniai šios sistemos sutrikimai būtų šalinami operatyviai, panaudojant visus turimus techninius resursus;

34.3. užtikrinti kompiuterinės įrangos apsaugą nuo kenksmingos programinės įrangos;

34.4. imtis priemonių, kad būtų užkirstas kelias atsitiktiniam ar neteisėtam vaizdo duomenų sunaikinimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam tvarkymui;

34.5. saugoti vaizdo duomenų įrašymo įrenginiuose esančius duomenis;

34.6. užtikrinti, kad stebėjimo priemonių vaizdas nebūtų prieinamas pašaliniais asmenims;

34.7. neatskleisti, neperduoti ir nesudaryti sąlygų bet kokiomis priemonėmis susipažinti su vaizdo duomenimis tam teisės neturintiems asmenims;

34.8. nedelsdamas pranešti Įstaigos vadovui apie bet kokią įtartina situaciją, kuri gali kelti grėsmę Įstaigos tvarkomų vaizdo duomenų saugumui;

34.9. laikytis kitų šiose Taisyklėse ir asmens duomenų apsaugą reglamentuojančiuose teisės aktuose nustatytų reikalavimų.

35. Įstaigos vadovo įgaliotas tvarkyti vaizdo duomenis asmuo turi teisę:

35.1. tiek stebėti tiesioginį kamerų vaizdą, tiek peržiūrėti įrašytus vaizdo įrašus, taip pat ištrinti, perkelti, nukopijuoti vaizdo įrašus, peržiūrėti darbuotojų judėjimo po Įstaigos teritoriją ir patalpas duomenis;

35.2. atlikti vaizdo stebėjimo sistemos priemonių techninę priežiūrą bei tikrinti įrašų kokybę. Šią teisę taip pat turi ir techninę priežiūrą atliekantys duomenų tvarkytojo darbuotojai;

35.3. kontroliuoti vaizdo stebėjimą, išskyrus atvejus, kai sistemoje yra techniniai gedimai arba atliekami profilaktiniai darbai.

36. Tiesioginį vaizdo įrašą gali stebėti:

36.1. Įstaigos vadovo įgalioti tvarkyti vaizdo duomenis darbuotojai.

37. Įgalioti asmenys ar kiti Įstaigos darbuotojai, pastebėję ar įtarę asmens duomenų saugumo pažeidimą, pastebėję, kad tvarkomi asmens duomenys tapo prieinami (kėsinais prie jų priėti) asmenų, kurie neturi teisės tvarkyti tvarkomų asmens duomenų, turi nedelsiant imtis visų įmanomų priemonių neteisėtai prieigai prie tvarkomų asmens duomenų nutraukti ir nedelsiant informuoti savo Įstaigos vadovą.

VII. REIKALAVIMAI DARBUOTOJAMS, TVARKANTIEMS ASMENS DUOMENIS IR JŲ ATSAKOMYBĖ

38. Darbuotojas, tvarkantis duomenų subjektų asmens duomenis, privalo:

38.1. laikytis pagrindinių asmens duomenų tvarkymo reikalavimų ir saugumo reikalavimų, įtvirtintų Lietuvos Respublikos teisinės apsaugos įstatyme, šiose taisyklėse ir kituose teisės aktuose;

38.2. Laikytis konfidencialumo principo ir laikyti paslapyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jis susipažino vykdydamas savo funkcijas, nebent tokia informacija būtų vieša pagal galiojančių įstatymų ar kitų teisės aktų nuostatas. Įstaigos darbuotojai, kurie tvarko asmens duomenis arba kuriems Įstaigos vadovo įsakymo pagrindu suteikti įgaliojimai ir / arba prieiga prie asmens duomenų, privalo pasirašyti Darbuotojo Įsipareigojimą saugoti asmens duomenis (Konfidencialumo pasižadėjimas). Pareiga saugoti asmens duomenų paslaptį galioja ir perėjus dirbti į kitas pareigas ar pasibaigus darbo santykiams;

38.3. laikytis taisyklėse nustatytų techninių ir organizacinių duomenų saugumo priemonių, kad būtų užkirstas kelias atsitiktiniam ar neteisėtam asmens duomenų sunaikinimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam tvarkymui, saugoti dokumentus, duomenų rinkmenas bei duomenų bazėse saugomus duomenis ir vengti nereikalingų kopijų darymo; Dokumentų kopijos, kuriose nurodomi duomenų subjekto duomenys, turi būti sunaikinamos tokiu būdu, kad šių dokumentų nebūtų galima atkurti ir atpažinti jų turinio;

38.4. neatskleisti, neperduoti ir nesudaryti sąlygų bet kokiomis priemonėmis susipažinti su asmens duomenimis nė vienam asmeniui, kuris nėra įgaliotas tvarkyti asmens duomenis;

38.5. nedelsiant pranešti tiesioginiam vadovui apie bet kokią įtartiną situaciją, kuri gali kelti grėsmę Įstaigos tvarkomų asmens duomenų saugumui;

38.6. laikytis kitų taisyklėse ir asmens duomenų apsaugą reglamentuojančiuose teisės aktuose nustatytų reikalavimų.

39. Darbuotojas netenka teisės tvarkyti asmens duomenis, kai pasibaigia jo darbo santykiai su Įstaiga arba kai jam pavedama vykdyti su duomenų tvarkymu nesusijusias funkcijas.

VIII. TECHNINĖS IR ORGANIZACINĖS ASMENS DUOMENŲ SAUGUMO PRIEMONĖS

40. Įstaiga, saugodama asmens duomenis, įgyvendina ir užtikrina tinkamas organizacines ir technines priemones, skirtas apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo. Nustačius asmens duomenų saugumo pažeidimus, Įstaiga imasi neatidėliotinių priemonių užkirsti kelią neteisėtam asmens duomenų tvarkymui.

41. Siekiant apsaugoti duomenų subjekto duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo nuo bet kokio kito neteisėto tvarkymo turi būti taikomos tokios organizacinės ir techninės priemonės:

41.1. Infrastruktūrinės priemonės: tinkamas techninės įrangos išdėstymas ir priežiūra, informacinių duomenų saugojimo priemonių fizinių ir programinių saugumo priemonių įgyvendinimas, griežtas priešgaisrinės apsaugos tarnybų nustatytų normų laikymasis ir kt.;

41.2. Administracinės priemonės: tinkamas darbo organizavimas, informacinių sistemų priežiūra;

41.3. Telekomunikacinės priemonės: tinklo valdymas, naudojimosi internetu saugumo užtikrinimas ir kt.

42. Įstaiga, atsižvelgiant į darbuotojo einamas pareigas, savo nuožiūra darbuotojams suteikia darbo priemones. Įstaigai 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 Įstaiga su darbuotoju nesutaria kitaip.

43. Darbuotojai neturi teisės savavališkai keisti jam priskirtos kompiuterinės įrangos (monitoriai, skeneriai spausdintuvai bei kopijavimo aparatų spausdinimo valdikliai, klaviatūros pelės, kolonėlės, ausinės, vaizdo kameros bei fotokameros, multimedijos projektoriai ir pan.) ir įdiegtos programinės įrangos.

44. Įstaigoje užtikrinamas patalpų, kuriose laikomi asmens duomenys saugumas ir priežiūra, priešgaisrinės saugos taisyklių laikymasis, įvairių techninių priemonių, būtinų asmens duomenų apsaugai užtikrinti, įgyvendinimas.

45. Darbuotojai privalo taip organizuoti savo darbą, kad kiek įmanoma apribotų galimybę kitiems asmenims (kitiems Įstaigos darbuotojams, praktikantams, savanorišką praktiką atliekantiems ar kitiems tretiesiems asmenims) sužinoti tvarkomus duomenis. Ši nuostata įgyvendinama:

45.1. nepaliekant dokumentų su tvarkomais asmens duomenimis ar kompiuterio, kuriuo naudojantis galima atidaryti rinkmenas su asmens duomenimis, be priežiūros taip, kad juose esančią informaciją galėtų perskaityti darbuotojai, neturintys teisės dirbti su konkrečiais asmens duomenimis ar kiti asmenys;

45.2. dokumentus laikyti taip, kad jų (ar jų fragmentų) negalėtų perskaityti kiti asmenys;

45.3. jei dokumentai, kuriuose 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 klientams, kitiems interesantams asmeniškai ir konfidencialiai.

46. Darbuotojai gali perduoti dokumentus, kuriuose nurodyti asmens duomenys, tik tiems darbuotojams, kurie pagal pareigas ar atskiru pavedimu turi teisę dirbti su asmens duomenimis.
47. Darbuotojai, kurie automatinio būdu tvarko asmens duomenis arba iš kurių kompiuterių galima patekti į Įstaigos informacines sistemas, kuriose yra saugomi asmens duomenys, savo kompiuteriuose turi naudoti slaptažodį. Slaptažodžiai neturi sutapti su darbuotojo ar jo šeimos narių asmeniniais duomenimis.
48. IT sistemos turi nustatyti sesijos laiką, t. y. naudotojui esant neaktyviam, neveiksniam sistemoje nustatyti laiką, jo sesija yra nutraukiama ne vėliau kaip po 15 minučių neaktyvios sesijos.
49. Kiekvienam Įstaigos darbuotojui suteikiamas unikalus prisijungimo prie Įstaigos tinklo resursų vardas ir slaptažodis. Darbuotojas, dirbantis konkrečiu kompiuteriu, gali žinoti tik savo slaptažodį, privalo saugoti slaptažodį ir neatskleisti jo tretiesiems asmenims.
50. Slaptažodžiai esant būtinybei (pasikeitus darbuotojui, iškilus įsilaužimo grėsmei ir pan.) turi būti keičiami periodiškai, o taip pat susidarius tam tikroms aplinkybėms (pvz. pasikeitus darbuotojui, iškilus įsilaužimo grėsmei, kilus įtarimui, kad slaptažodis tapo žinomas tretiesiems asmenims, ir pan.)
51. Visuose kompiuteriuose, kurie įjungiami į kompiuterių tinklą, turi nuolat veikti antivirusinė programa su naujausia virusų aprašymo duomenų baze.
52. Darbuotojų kompiuteriai, kuriuose saugomos rinkmenos su fizinių asmenų duomenimis, negali būti laisvai prieinami iš kitų tinklo kompiuterių. Šių kompiuterių antivirusinė įranga turi būti nuolat atnaujinama.
53. Darbuotojams, naudojančiams elektroninį paštą, interneto prieigą ir kitą informacinių technologijų ir telekomunikacijų įrangą, draudžiama:
- 53.1. siųsti elektroninio pašto žinutes, naudojantis kito asmens arba neegzistuojančiu elektroninio pašto adresu;
- 53.2. siųsti elektroninio pašto žinutes, nuslepiančias savo tapatybę;
- 53.3. negavus Įstaigos vadovo sutikimo, siųsti elektroninius laiškus, kuriuose yra informacija pripažįstama konfidencialia informacija ar Įstaigos komercine paslaptimi, išskyrus, jei informacija siunčiama asmeniui, kuris turi teisę gauti šią informaciją;
- 53.4. negavus Įstaigos vadovo sutikimo perduoti, platinti, atskleisti tretiesiems asmenims darbu su technine ir programine įranga jiems suteiktus prieigos vardus, slaptažodžius ar kitus duomenis;
- 53.5. kurti ar platinti laiškus, skatinančius gavėją siųsti laiškus kitiems. Laiškai su perspėjimais dėl kompiuterių virusų, telefonų pasiklausymų ar kitų tariamų reiškinų, kuriuose prašoma nusiųsti gautą laišką visiems savo kolegoms, draugams ar pažįstamiems, turi būti nedelsiant ištrinami. Jei pranešimas sukelia įtarimų, prieš jį pašalinant, pranešti tiesioginiam arba Įstaigos vadovui;
- 53.6. naudojant interneto prieigą ir elektroninį paštą asmeniniams tikslams, Lietuvos Respublikos įstatymais draudžiamai veiklai, šmeižiančio, įžeidžiančio, grasinančiojo pobūdžio ar visuomenės dorovės ir moralės principams prieštaraujantčiai informacijai „spam“ siųsti ar kitiems tikslams, galintiems pažeisti Įstaigos ar kitų asmenų teisėtus interesus;
- 53.7. atlikti veiksmus, pažeidžiančius fizinio ar juridinio asmens teises, kurias saugo autorių, gretutinių ir intelektualios nuosavybės teisių apsaugos įstatymai. Tarp tokių veiksmų yra programinės

įrangos diegimas, naudojimas, saugojimas arba platinimas neturint licencijos, neleistinas autorių teisėmis apsaugotų kūrinių kopijavimas;

53.8. 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 kompiuterių ar telekomunikacinių įrenginių bei programinės įrangos funkcionavimą ir saugumą;

53.9. atskleisti prisijungimo prie Įstaigos sistemų informaciją (prisijungimo vardą, slaptažodį) arba leisti naudotis savo prisijungimo vardu kitiems asmenims;

53.10. Dirbant su slaptažodžiais reikia laikytis taisyklių:

53.10.1. saugoti slaptažodį. Neužrašinėti jo ant popieriaus skiaučių, kalendorių ir pan. Nepalikti lapelio su slaptažodžiu priklijuoto prie vaizduoklio arba prie apatinės darbo stalo pusės;

53.10.2. nenaudoti trumpų ir elementarių slaptažodžių sudarytų iš reikšminių žodžių;

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

53.12. ardyti ar išmontuoti ar kitaip keisti kompiuterinę įrangą;

53.13. perkopijuoti programinę įrangą;

53.14. savarankiškai šalinti kompiuterinės įrangos gedimus;

53.15. parsisiųsti ar žaisti internetinius ar kitus kompiuterinius žaidimus;

53.16. savavališkai blokuoti antivirusines programas ar kitas programas;

53.17. sutrikdyti kompiuterinės sistemos darbą arba panaikinti galimybę naudotis teikiama paslauga ar informacija;

53.18. dalyvauti interneto lažybose ir azartiniuose lošimuose;

53.19. naudoti Įstaigos išteklius komercinei veiklai vystyti ar naudai gauti;

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

53.21. pažeisti kitų tinklų, kurių paslaugomis naudojamasi, naudojimo arba ekvivalentiškas taisykles;

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

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

53.24. neįgaliotiems asmenims Įstaigoje ar už Įstaigos naudoti ir perduoti slaptažodžius ir kitus duomenis, kuriais pasinaudojus programinėmis ir techninėmis priemonėmis galima sužinoti Įstaigos duomenis ar kitaip sudaryti sąlygas susipažinti su Įstaigos duomenimis.

54. Keitimosi informacija politika:

54.1. Perduodant informaciją elektroniniu paštu, būtina:

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

54.1.2. už organizacijos ribų siunčiamiems laiškam naudoti el. pašto programoje el. laiško parašą (signature) ir jo nekeisti;

54.1.3. priimant sprendimus pagal elektroniniu paštu gautą informaciją, būtina įsitikinti šios informacijos tikrumu (kitas asmuo gali apsimesti tikruoju siuntėju). Kilus įtarimui bei svarbiais atvejais rekomenduojama susisiekti su siuntėju ir įsitikinti ar gautas laiškas buvo jo išsiųstas;

54.2. Neatverti pridėtų (angl. „attached“) failų, kurie yra gauti iš nepažįstamų asmenų, arba nėra galimybės įsitikinti šių failų turiniu;

54.3. Už pašalinių asmenų naudojimąsi internetu kompiuteryje ir informacijos perdavimą elektroniniu paštu yra atsakingas kompiuterio naudotojas.

55. Bendros apsaugos nuo virusų taisyklės:

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

55.2. kilus įtarimui patikrinti kompiuterį nuo virusų;

55.3. siekiant išvengti kompiuterinių virusų, nepaleisti nežinomų programų. Gavus nežinomų siuntėjų atsiųstų elektroninių laiškų priedus, kuriuose gali būti kompiuterių virusų, darbuotojas privalo neatidaryti gautų elektroninių laiškų priedų ir informuoti tiesioginį arba Įstaigos vadovą;

55.4. darbuotojas, pastebėjęs virusų atakos požymius, privalo išjungti kompiuterį ir kreiptis į tiesioginį arba Įstaigos vadovą.

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

57. Įstaiga pasilieka teisę be atskiro darbuotojo įspėjimo riboti prieigą prie atskirų interneto svetainių ar programinės įrangos. Nepakankant minėtų priemonių, Įstaiga gali tikrinti, kaip darbuotojas laikosi elektroninio pašto ir interneto resursų naudojimo reikalavimų nurodytais tikslais, tiriant incidentus, atiduoti darbuotojų naudojamą įrangą tirti tretiesiems asmenims, kurie teisės aktų nustatyta tvarka turi teisę tokius duomenis gauti.

58. Įstaiga neužtikrina darbuotojų asmeninės informacijos konfidencialumo darbuotojams, naudojančiams elektroninį paštą ir interneto resursus asmeniniais tikslais. Įstaiga turi teisę neįspėjus darbuotojo atidaryti šiam priskirtą darbinę elektroninio pašto dėžutę ir skaityti elektroninius laiškus tada, jei yra pagrindo manyti, kad darbuotojo elektroninio pašto dėžutėje yra netinkamo, įstatymus ar Įstaigos teisės interesus pažeidžiančio turinio informacija arba egzistuoja teisėta su darbo santykiais susijusi priežastis atlikti šiuos veiksmus.

59. Įstaigos vadovas neužtikrina, kad bus išsaugotas privatumas to, ką Įstaigos darbuotojai sukuria, siunčia ar gauna Įstaigos informacinėje sistemoje.

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

**IX. ASMENS DUOMENŲ TVARKYMOUI TAIKOMŲ SAUGUMO
PRIEMONIŲ SĄRAŠAS**

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

29	patalpose yra ugnies gesintuvai;
30	pastato patalpose įrengti dūmų ir temperatūros jutikliai;
31	stebima elektros srovės tiekimo būklė;
32	kabėliai yra izoliaciniuose vamzdėiuose;
33	elektros ir duomenų kabėliai saugiai atskirti.

X. ASMENS DUOMENŲ TVARKYTOJAI IR GAVĖJAI

61. Tais atvejais, kai Įstaiga įgalioja duomenų tvarkytoją atlikti asmens duomenų tvarkymo veiksmus, tarp įstaigos ir duomenų tvarkytojo turi būti sudaroma duomenų tvarkymo sutartis.
62. Įstaiga, sutartimi įgaliodama duomenų tvarkytoją tvarkyti asmens duomenis, nurodo, kad asmens duomenys būtų tvarkomi atsižvelgiant į asmens duomenų tvarkymą reglamentuojančius teisės aktus, Įstaigos nurodymus, taip pat nurodant, kokius asmens duomenų tvarkymo veiksmus privalo atlikti duomenų tvarkytojas Įstaigos vardu, duomenų tvarkytojo įsipareigojimais Įstaigai, įskaitant įsipareigojimą laikytis ADTAI įtvirtintų reikalavimų, duomenų subjektų kategorijos, duomenų tvarkytojo pareiga ištrinti arba grąžinti Įstaigai asmens duomenis, jų kopijas, pabaigus Įstaigai teikti paslaugas.
63. Įstaiga, sudarydama sutartį su duomenų tvarkytoju, be kita ko, nurodo, kad duomenų tvarkytojas privalo užtikrinti Įstaigos perduodamų tvarkyti duomenų konfidencialumą, o ketindamas tvarkymui pasitelkti trečiuosius asmenis (kitus duomenų tvarkytojus), duomenų tvarkytojas privalo gauti išankstinį rašytinį Įstaigos pritarimą.
64. Duomenų valdytojo tvarkomi duomenys duomenų gavėjams, kurie po duomenų perdavimo asmens duomenis tvarko savarankiškais tikslais, o ne pagal duomenų valdytojo nurodymus, teikiami tokią pareigą teikti duomenis numatant teisės aktui, esant duomenų subjekto sutikimui arba kitam teisėto duomenų teikimo (tvarkymo) pagrindui.
65. Duomenų teikimas duomenų gavėjui turi būti būtinas pasiekti duomenų tvarkymo tikslui, nustatytam prieš renkant duomenis, arba turi egzistuoti tinkamas teisinis pagrindas duomenis tvarkyti ir teikti nauju tikslu.
66. Duomenų valdytojo įgaliotų duomenų tvarkytojų ir jų atliekamų funkcijų, taip pat duomenų gavėjų sąrašas pateikiamas Tvarkymo veiklos įrašuose. Pasitelkus naują duomenų tvarkytoją ar pradėjus teikti duomenis naujam duomenų gavėjui, Tvarkymo veiklos įrašas papildomas nauja informacija. Atitinkamai, atsisakius duomenų tvarkytojo paslaugų ar pasikeitus duomenų gavėjui, taip pat padaromi atitinkami pokyčiai Tvarkymo veiklos įrašuose.

XI. DUOMENŲ SUBJEKTŲ TEISĖS IR JŲ ĮGYVENDINIMO TVARKA

67. Duomenų subjektai turi šias teises:

67.1. Susipažinti su savo asmens duomenimis:

67.1.1. duomenų subjektas turi teisę susipažinti su jo tvarkomais duomenimis, tvarkymo tikslais, saugojimo laikotarpiu, savo teisėmis, informacija ar naudojamas automatizuotas sprendimų priėmimas, įskaitant profiliavimą bei jo loginį pagrindimą;

67.1.2. duomenų subjektui turi būti atskleisti visi duomenų gavėjai ar jų kategorijos, kuriems jau buvo arba bus atskleisti duomenys;

67.1.3. tvarkomus duomenis duomenų subjektui teikti raštu ir neatlygintinai. Tam tikrais atvejais (kai duomenų subjektas akivaizdžiai piktnaudžiauja savo teisėmis, nepagrįstai arba neproporcingai, pakartotinai teikia prašymus dėl jų pasikartojančio turinio pateikti informaciją, išrašus, dokumentus), toks informacijos ir duomenų teikimas duomenų subjektui gali būti apmokestintas, t. y. duomenų valdytojas gali imti pagrįstą mokesį, atsižvelgdamas į informacijos teikimo arba pranešimų ar veiksmų, kurių prašoma, administracines išlaidas; arba gali atsisakyti imtis veiksmų pagal prašymą. Duomenų valdytojui tenka pareiga įrodyti, kad prašymas yra akivaizdžiai nepagrįstas arba neproporcingas;

67.1.4. informaciją pateikti įprastai naudojama elektronine forma, nebent prašoma informaciją pateikti kitaip.

67.2. Reikalauti ištaisyti netikslius duomenis ar papildyti neišsamius duomenis:

67.2.1. duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas nepagrįstai nedelsdamas ištaisyty netikslius su juo susijusius asmens duomenis. Atsižvelgiantį tikslus, kuriais duomenys buvo tvarkomi, duomenų subjektas turi teisę reikalauti, kad būtų papildyti neišsamūs asmens duomenys pateikdamas papildomą prašymą;

67.2.2. kiekvienam duomenų gavėjui, kuriam buvo atskleisti asmens duomenys, duomenų valdytojas praneša apie bet kokią asmens duomenų ištaisymą, ištrynimą arba tvarkymo apribojimą, nebent to padaryti nebūtų įmanoma arba tai pareikalautų neproporcingų pastangų. Duomenų subjektui paprašius, duomenų valdytojas informuoja duomenų subjektą apie tuos duomenų gavėjus.

67.3. Nesutikti, kad būtų tvarkomi jo asmens duomenys:

67.3.1. duomenų subjektas turi teisę dėl su jo konkrečiu atveju susijusių priežasčių bet kuriuo metu nesutikti, kad su susiję asmens duomenys būtų tvarkomi, įskaitant profiliavimą. Duomenų valdytojas nebetvarko asmens duomenų, išskyrus atvejus, kai duomenų valdytojas įrodo, kad duomenys tvarkomi dėl teisinių priežasčių, kurios yra viršesnės už duomenų subjekto interesus, teises ir laisves, arba siekiant pareikšti, vykdyti ar apginti teisinius reikalavimus;

67.3.2. kai asmens duomenys tvarkomi tiesioginės rinkodaros tikslais, duomenų subjektas turi teisę bet kuriuo metu nesutikti, kad su juo susiję asmens duomenys būtų tvarkomi tokios rinkodaros tikslais, įskaitant profiliavimą, kiek jis susijęs su tokia rinkodara;

67.3.3. duomenų subjektas apie teisę nesutikti aiškiai informuojamas ne vėliau kaip pirmą kartą susisiekiant su duomenų subjektu, ir ši informacija pateikiama aiškiai ir atskirai nuo visos kitos informacijos.

67.4. Reikalauti ištrinti duomenis („Teisė būti pamirštam“):

67.4.1. Duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas nepagrįstai nedelsdamas išmintų su juo susijusius asmens duomenis, o duomenų valdytojas yra įpareigotas nepagrįstai nedelsdamas ištrinti asmens duomenis, jei tai galima pagrįsti viena iš šių priežasčių:

67.4.1.1. kai asmens duomenys nebėra reikalingi, kad būtų pasiekti tikslais, kuriais jie buvo renkami arba kitaip tvarkomi;

67.4.1.2. kai asmens duomenų subjektas atšaukia sutikimą ir nėra jokio teisinio pagrindo tvarkyti duomenis;

67.4.1.3. kai asmens duomenų subjektas nesutinka su duomenų tvarkymu ir nėra viršesnių teisėtų priežasčių tvarkyti duomenis;

67.4.1.4. kai asmens duomenys buvo tvarkomi neteisėtai;

67.4.1.5. kai asmens duomenys turi būti ištrinti dėl duomenų valdytojui nustatytos teisinės prievolės;

67.4.1.6. kai asmens duomenys buvo surinkti informacinės visuomenės paslaugų siūlymo kontekste.

67.5. Teisė į duomenų perkėliamumą:

67.5.1. Duomenų subjektas turi teisę gauti su juo susijusius asmens duomenis, kuriuos jis pateikė duomenų valdytojui susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu, ir turi teisę persiųsti tuos duomenis kitam duomenų valdytojui, o duomenų valdytojas, kuriam asmens duomenys buvo pateikti, turi nesudaryto tam kliūčių, kai:

67.5.1.1. duomenų tvarkymas yra grindžiamas sutikimu arba sutartimi;

67.5.1.2. duomenys tvarkomi automatizuotomis priemonėmis;

67.5.2. Naudodamasis savo teise į duomenų perkėliamumą, duomenų subjektas turi teisę, kad vienas duomenų valdytojas asmens duomenis tiesiogiai persiųstų kitam, kai tai techniškai įmanoma;

67.5.3. Šia teise naudojama nedarant poveikio teisei reikalauti ištrinti duomenis („Teisei būti pamirštam“);

67.5.4. Teisė į duomenų perkėliamumą negali daryti neigiamo poveikio kitų teisėms ir laisvėms.

67.6. Teisė apriboti asmens duomenų tvarkymą:

67.7. Duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas apribotų duomenų tvarkymą kai taikomas vienas iš šių atvejų:

67.7.1. asmens duomenų subjektas užginčija duomenų tikslumą tokiam laikotarpiui, per kurį duomenų valdytojas gali patikrinti asmens duomenų tikslumą;

67.7.2. asmens duomenų tvarkymas yra neteisėtas ir duomenų subjektas nesutinka, kad duomenys būtų ištrinti, ir vietoj to prašo apriboti jų naudojimą;

67.7.3. duomenų valdytojui nebereikia asmens duomenų tvarkymo tikslais, tačiau jų reikia duomenų subjektui siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus;

67.7.4. duomenų subjektas paprieštaravo duomenų tvarkymui, kol bus patikrinta, ar duomenų valdytojo teisėtos priežastys yra viršesnės už duomenų subjekto priežastis.

67.8. Kai duomenų tvarkymas yra apribotas pagal aukščiau išvardintus punktus, išskyrus saugojimą, tik gavus duomenų subjekto sutikimą arba siekiant pareikšti, vykdyti arba apginti teisinius

reikalavimus, arba apsaugoti kito fizinio ar juridinio asmens teises, arba dėl valstybės narės viešojo intereso priežasčių.

67.9. Duomenų subjektą, kuris pasiekė, kad būtų apribotas duomenų tvarkymas pagal aukščiau išvardintus punktus, duomenų valdytojas informuoja prieš panaikinant apribojimą tvarkyti duomenis.

68. Įstaiga imasi tinkamų priemonių, jog informacija susijusi su duomenų tvarkymu, duomenų subjektui būtų pateikta glausta, skaidria, suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba.

69. Duomenų subjektas dėl jo teisių įgyvendinimo privalo pateikti Įstaigai rašytinį prašymą, kuris turi būti:

69.1. įskaitomas, duomenų subjekto pasirašytas, naudojant laisvą prašymo formą ir formatą arba naudojant rekomenduojamą Įstaigos parengtą kreipimosi formą;

69.2. prašyme turi būti nurodyta: duomenų subjekto vardas, pavardė, kiti požymiai, leidžiantys identifikuoti asmenį, kontaktiniai duomenys ir informacija apie tai, kokią iš anksčiau nurodytų teisių ir kokios apimties duomenų subjektas pageidauja įgyvendinti, bei informacija, koku būdu pageidauja gauti atsakymą.

70. Prašymą galima pateikti:

70.1. asmeniškai;

70.2. paštu ar per pasiuntinį;

70.3. per atstovą;

70.4. elektroninių ryšių priemonėmis.

71. Įstaiga, duomenų subjekto prašymo, kuris pateiktas nesilaikant šiose Taisyklėse nustatytų reikalavimų, nenagrinėja.

72. Pateikdamas prašymą, duomenų subjektas privalo patvirtinti savo tapatybę:

72.1. kai prašymas teikiamas tiesiogiai atvykus į Įstaigą - pateikti galiojantį asmens tapatybę patvirtinantį dokumentą;

72.2. kai prašymas siunčiamas paštu ar per pasiuntinį - pridėti notaro ar kita Lietuvos teisės nustatyta tvarka patvirtintą prašymą teikiančio asmens tapatybę patvirtinančio dokumento kopiją;

72.3. kai prašymas teikiamas per atstovą - pateikti Lietuvos Respublikos teisės aktų nustatyta tvarka atstovavimą patvirtinantį dokumentą ar įstatymų nustatyta tvarka patvirtintą atstovavimo dokumento kopiją;

72.4. kai prašymas teikiamas elektroninių ryšių priemonėmis - pasirašyti kvalifikuotu elektroniniu parašu.

73. Jei įmanoma, duomenų subjekto prašymu, informacija gali būti suteikta žodžiu, jeigu duomenų subjekto tapatybę galima įsitikinti patikrinus duomenų subjekto nurodytą ir Įstaigos turimą informaciją (pavyzdžiui: vardas, pavardė, telefono numeris gali būti pasakomi duomenų subjektui, jeigu duomenų subjektas prašo šią informaciją suteikti žodžiu, kreipdamasis į Įstaigą, ir jeigu yra techninė galimybė šią informaciją surinkti).

74. Visi prašymai, kuriuos Įstaiga bet kokiomis ryšio priemonėmis gauna dėl duomenų subjektų teisių įgyvendinimo turi būti perduoti ar persiųsti Pareigūnui. Visi Įstaigos darbuotojai, kurie prižiūri įeinančią komunikaciją, privalo užtikrinti, kad gauti duomenų subjektų prašymai būtų atpažinti ir perduoti Pareigūnui ir Įstaigos vadovo įgaliotam darbuotojui nedelsiant, ne vėliau kaip per 1 (vieną) darbo dieną.

75. Duomenų subjektų teisių įgyvendinimo tvarka:

75.1. Duomenų valdytojas privalo suteikti duomenų subjektui informaciją:

75.1.1. per pagrįstą laikotarpį nuo asmens duomenų gavimo, bet **ne vėliau kaip per vieną mėnesį nuo duomenų subjekto prašymo gavimo dienos**, atsižvelgiant į konkrečias asmens duomenų tvarkymo aplinkybes;

75.1.2. jeigu asmens duomenys bus naudojami ryšiams su duomenų subjektu palaikyti – **ne vėliau kaip pirmą kartą susisiekiant su tuo duomenų subjektu**;

75.1.3. jeigu numatoma asmens duomenis atskleisti kitam duomenų gavėjui – **ne vėliau kaip atskleidžiant duomenis pirmą kartą**.

75.2. Duomenų valdytojas nepagrįstai nedelsdamas, tačiau bet kuriuo atveju **ne vėliau kaip per vieną mėnesį nuo prašymo gavimo**, pateikia duomenų subjektui informaciją (atsakymą) apie veiksmus, kurių imtasi gavus prašymą. Šis laikotarpis prireikus gali būti pratęstas dar **dviem mėnesiams**, atsižvelgiant į prašymų sudėtingumą ir skaičių. Duomenų valdytojas **per vieną mėnesį nuo prašymo gavimo** informuoja duomenų subjektą apie tokį pratęsimą, kartu pateikdamas vėlavimo priežastis. Kai duomenų subjektas prašymą pateikia elektroninės formos priemonėmis, informacija jam taip pat pateikiama, jei įmanoma, elektroninėmis priemonėmis, išskyrus atvejus, kai duomenų subjektas paprašo ją pateikti kitaip.

75.3. Jei duomenų valdytojas nesiima veiksmų pagal duomenų subjekto prašymą, duomenų valdytojas nedelsdamas, tačiau **ne vėliau kaip per vieną mėnesį nuo prašymo gavimo**, informuoja duomenų subjektą apie neveikimo priežastis ir apie galimybę pateikti skundą Priežiūros institucijai bei pasinaudoti teisių gynimo priemone.

76. Gavus duomenų subjekto kreipimąsi dėl jo asmens duomenų neteisingumo, neišsamumo, netikslumo Įstaigos atsakingas asmuo nedelsdamas patikrina asmens duomenis ir duomenų subjekto rašytiniu prašymu, pateiktu asmeniškai, paštu ar elektroninių ryšių priemonėmis, patikrinus / įsitikinus Duomenų subjekto tapatybę ir Asmens duomenis patvirtinančių dokumentų atitiktį / atitiktimi teisės aktų reikalavimams, nedelsdamas privalo ištaisyti neteisingus, neišsamius, netikslus Asmens duomenis arba sustabdo tokių duomenų tvarkymo veiksmus, išskyrus saugojimą.

77. Gavus duomenų subjekto kreipimąsi dėl jo duomenų tvarkymo neteisėtumo, nesąžiningumo Įstaigos atsakingas asmuo nedelsdamas patikrina duomenų tvarkymo teisėtumą, nesąžiningumą ir, gavus rašytinį prašymą, patikrinus / įsitikinus asmens dokumentų atitiktį / atitiktimi teisės aktų reikalavimams, nedelsdamas sunaikina neteisėtai ir nesąžiningai sukauptus asmens duomenis ar sustabdo tokių duomenų tvarkymo veiksmus, išskyrus saugojimą. Duomenų subjekto pateikta informacija bei visi atlikti tolimesni veiksmai su šia informacija dokumentuojami „Neatitikčių registravimo žurnale“ šių Taisyklių skyriuje „Neatitikčių, incidentų ir korekcinų veiksmų valdymas“ nustatyta tvarka.

78. Duomenų subjektams teikiama informacija, duomenų subjekto teisių įgyvendinimas ir visi su tuo susiję pranešimai bei visi veiksmai yra nemokami. Kai duomenų subjekto prašymai yra akivaizdžiai nepagrįsti arba neproporcingi, visų pirma dėl jų pasikartojančio turinio, Įstaiga gali imti

pagrįstą mokestį, atsižvelgdama į informacijos teikimo ir pranešimų ar veiksmų, kurių prašoma, administracines išlaidas; arba gali atsisakyti imtis veiksmų pagal duomenų subjekto prašymą.

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

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

80. 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.

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

81.1. keltų didelį pavojų duomenų subjektų teisėms ir laisvėms (pavyzdžiui, atvejai, kai duomenų subjektas neturi galimybės nesutikti su duomenų tvarkymu, duomenys perduodami už ES ribų, būtų pradėti tvarkyti duomenys, kurie gauti juos sujungus su duomenimis iš kitų šaltinių, būtų tvarkomi jautrūs duomenys, tokie kaip sveikata, būtų pradėti naudoti nauji technologiniai sprendimai, pavyzdžiui, veido atpažinimo sistemos, ar kitų biometrinių duomenų atpažinimo ir kt.);

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

81.3. būtų pradėtas vykdyti sistemingas vaizdo stebėjimas dideliu mastu;

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

82. PDAV nereikia atlikti šiais atvejais:

82.1. kai duomenų tvarkymas negali kelti didelio pavojaus fizinių asmenų teisėms bei laisvėms;

82.2. kai duomenų tvarkymo pobūdis, aprėptis, kontekstas ir tikslai yra panašūs į duomenų tvarkymą, kurio PDAV buvo atliktas;

82.3. kai duomenų tvarkymas teisės aktuose įtrauktas į neprivalomą duomenų tvarkymo operacijų sąrašą;

82.4. kitais teisės aktuose nustatytais atvejais.

83. PDAV taip pat gali būti atliekamas ir šiame skyriuje neaptais atvejais, bet esant Įstaigos vadovo sprendimu tai atlikti.

84. PDAV atlieka Įstaigos vadovo įsakymu sudaroma darbo grupė iš Įstaigos darbuotojų arba PDAV atlieka asmenys pagal paslaugų teikimo sutartį.

85. Įstaigos vadovo įsakymu sudaromai darbo grupei paskiriamas jos vadovas atlikti PDAV. Į jos sudėtį gali būti įtrauktas ir Pareigūnas arba gali būti konsultuojamasi su Pareigūnu.

86. Darbo grupė PDAV metu pildo Priežiūros institucijos rekomenduojamą PDAV formą (toliau – Forma).

87. Užpildyta ir pasirašyta Forma teikiama Įstaigos vadovui, kuris priima sprendimus dėl tolimesnio asmens duomenų tvarkymo.

88. Kai iš PDAV paaiškėja, kad duomenų tvarkymo operacijos kelia didelį pavojų duomenų subjektų teisėms ir laisvėms, o Įstaiga negali jo sumažinti tinkamomis rizikos valdymo priemonėmis (turimomis technologijomis ir įgyvendinimo sąnaudomis), prieš pradėdant asmens duomenų tvarkymą turi būti iš anksto konsultuojamasi su Priežiūros institucija.

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

XIII. NEATITIKČIŲ, INCIDENTŲ IR KOREKCINIŲ VEIKSMŲ VALDYMAS

90. Neatitikčių identifikavimas:

90.1. Neatiktys gali būti identifikuotos:

90.1.1. vykdant kasdieninę veiklą;

90.1.2. kontroliuojančių institucijų patikrinimo metu;

90.1.3. gavus informaciją iš asmens duomenų subjektų;

90.1.4. kitu būdu.

90.2. Neatiktis gali nustatyti / informaciją apie neatiktis gali gauti bet kuris Įstaigos darbuotojas.

91. Neatikties tipai:

91.1. Suinteresuotų šalių skundai dėl galimai netinkamai tvarkomų asmens duomenų. Suinteresuotos šalys – tai visi duomenų subjektai, kurių asmens duomenis Įstaiga tvarko.

91.2. Neatiktys susijusios su programine įranga ir jos gedimais.

91.3. Neatiktys susijusios su technine įranga.

91.4. Informacijos saugumo įvykiai ir incidentai.

91.5. Kontroliuojančių institucijų radiniai – Priežiūros institucija, priešgaisrinės saugos departamento ar kitų kontroliuojančių institucijų pastebėti trūkumai.

91.6. Kita – aukščiau nepaminėtos neatiktys susijusios su asmens duomenų tvarkymu, kurias sąlygoja darbuotojų kompetencijos stoka, ar kitos priežastys nepaminėtos Taisyklėse.

92. Neatitikčių valdymas:

92.1. Informaciją apie neatiktį gavęs ar neatiktį pastebėjęs darbuotojas nedelsdamas perduoda informaciją Įstaigos vadovui, Pareigūnui arba Įstaigos vadovo įgaliotam darbuotojui, kuris:

92.1.1. dokumentuoja identifikuotą neatiktį „Neatitikčių registravimo žurnale“ (Taisyklių priedas Nr. 3);

92.1.2. įvertina neatikties įtaką Įstaigai ir Įstaigos tvarkomų asmens duomenų saugumui, jos sprendimo sudėtingumą;

92.1.3. paskiria atsakingus asmenis neatikties priežastiai bei neatitikčių šalinimo veiksams nustatyti ir įgyvendinti, kartu su atsakingais asmenimis aptaria neatikties šalinimo veiksnius bei terminus, duoda atitinkamas instrukcijas paskirtiems darbuotojams dėl jų pareigų, funkcijų atlikimo, susijusio su asmens duomenų incidento valdymu.

92.2. Įgyvendinus suplanuotus veiksmus, Pareigūnas arba Įstaigos vadovo įgaliotas darbuotojas patikrina atliktų veiksmų rezultatyvumą. Tais atvejais kai atlikti veiksmai yra rezultatyvūs, „Neatitikčių registravimo žurnale“ (Taisyklių priedas Nr. 3) fiksuojamas neatikties statusas „uždaryta“. Jeigu atlikti veiksmai nėra rezultatyvūs, paskirti atsakingi darbuotojai toliau planuoja ir įgyvendina neatitikčių šalinimo veiksmus, iki jie bus rezultatyvūs.

92.3. Apie visus įgyvendintus neatitikčių valdymo veiksmus ir jų rezultatyvumą Pareigūnas arba Įstaigos vadovo įgaliotas darbuotojas informuoja Įstaigos vadovą.

92.4. Pareigūnas arba Įstaigos vadovo įgaliotas darbuotojas, tvarkantis asmens duomenis kartu su nustatytos neatikties šalinime dalyvavusiais darbuotojais parengia planą su prevenciniais veiksmais, kuriais būtų siekiama ateityje užkirsti kelią pasikartoti analogiškam ar

panašiam incidentui ir pateikia jį Įstaigos vadovui, kuris toliau priima sprendimą dėl numatytų priemonių įgyvendinimo.

93. Jei dėl įvykdyto asmens duomenų incidento kyla pavojus duomenų subjektų teisėms ir laisvėms, Pareigūnas ar kitas Įstaigos vadovo paskirtas darbuotojas privalo **nedelsiant, bet ne vėliau nei kaip per 72 val.** pranešti VDAI apie įvykusį incidentą. Kilus ypatingai dideliam pavojui duomenų subjektų teisėms ir laisvėms, informacija apie įvykusį incidentą nedelsiant taip pat turi būti pateikta duomenų subjektams. Nesant galimybės informuoti visus duomenų subjektus dėl jų didelio kiekio ar kitų priežasčių, Pareigūnas ar kitas Įstaigos vadovo paskirtas darbuotojas kartu su Įstaigos vadovu apsvarsto ir priima sprendimą šią informaciją pateikti per visuomenės informavimo kanalus (spauda, televizija, kt.).

94. Teikiant pranešimą dėl įvykusio asmens duomenų incidento, VDAI, duomenų subjektams privalo būti trumpai aprašytas asmens duomenų incidento pobūdis, nurodant apytikslį duomenų subjektų skaičių, kurių asmens teisės ir laisvės galėjo būti pažeistos, Pareigūno arba Įstaigos vadovo įgalioto darbuotojo kontaktai, trumpai aprašytos tikėtinos incidento pasekmės bei priemonės, kurių Įstaiga imasi / imsis, kad būtų pašalintos neigiamos pasekmės, susijusios su įvykusiu incidentu.

95. Nustatant, ar būtina vykdyti informavimo pareigą, Pareigūnas ar kitas Įstaigos vadovo įgaliotas darbuotojas privalo įvertinti, ar dėl įvykusio incidento:

95.1. įvyko konfidencialumo pažeidimas (pavyzdžiui, atskleisti duomenys ir jie tapo prieinami tretiesiems asmenims, suteikiant prieigą, tinkamai nešifruojant, kt.);

95.2. įvyko duomenų pasiekiamumo pažeidimas (pavyzdžiui prarasti duomenys ir neturima atsarginių kopijų);

95.3. įvyko duomenų vientisumo pažeidimas (pavyzdžiui, prarasti klientų duomenys, turima tik dalis atsarginių kopijų, dėl ko neįmanoma „atkurti“ visos su klientu bendravimo istorijos).

96. Informavimas gali vykti ir esant kitiems pagrindams, jei tokius nustato Įstaiga ir / ar Pareigūnas.

97. Pareigūnas ar kitas Įstaigos vadovo įgaliotas darbuotojas privalo užtikrinti, kad visos neatitiktys, įskaitant ir asmens duomenų apsaugos incidentus būtų tinkamai dokumentuotos ir saugomos.

XIV. ASMENS DUOMENŲ APSAUGOS PAREIGŪNAS

98. Įstaigos vadovo įsakymu, Pareigūnas gali būti paskirtas iš esamų Įstaigos darbuotojų, naujas darbuotojas arba asmuo, su kuriuo būtų sudaroma paslaugų teikimo sutartis.

99. 2. Įstaigos vadovas paskyręs arba sudaręs su Pareigūnu paslaugų teikimo sutartį, privalo užtikrinti, kad Pareigūno kontaktiniai duomenys per protingą terminą nuo jo paskyrimo / paslaugų sutarties sudarymo būtų tinkamai paskelbti duomenų subjektams bei pranešti VDAI.

100. Skirdamas Pareigūną, Įstaigos vadovas privalo įvertinti ir įgyvendinti tai, kad:

100.1. Pareigūnas turėtų tinkamų asmens duomenų teisinės apsaugos praktinių ir ekspertinių žinių;

100.2. Pareigūnas būtų įtraukiamas į visų su asmens duomenų apsauga ir privatumu susijusių klausimų nagrinėjimą Įstaigoje;

100.3. Pareigūnas būtų tiesiogiai pavaldus Įstaigos vadovui;

100.4. Pareigūnas neturėtų jokių kitų pareigų, neatliktų funkcijų, kurios galėtų sukelti interesų konfliktą su jo atliekamomis Pareigūno funkcijomis.

101. Pareigūnas privalo:

101.1. užtikrinti, kad Įstaigoje 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;

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

101.3. konsultuoti ir stebėti, kaip Įstaigoje atliekamas poveikio duomenų apsaugai vertinimas;

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

101.5. informuoti Įstaigos vadovą apie bet kokius neatitikimus, pažeidimus asmens duomenų apsaugos srityje, kuriuos Pareigūnas nustato, vykdydamas savo funkcijas;

101.6. mokyti Įstaigos darbuotojus, dirbančius su asmens duomenimis, asmens duomenų teisinės apsaugos klausimais;

101.7. bendradarbiauti, būti kontaktiniu asmeniu santykiuose su VDAI.

102. Pareigūnas savo pareigas ir užduotis atlieka nepriklausomai. Įstaigos vadovas, ir jokie kiti Įstaigos darbuotojai Pareigūnui negali teikti jokių nurodymų dėl jo užduočių vykdymo.

103. Pareigūnas turi teisę naudotis Įstaigos teisės, personalo, informacinių technologijų, kitų padalinių pagalba, prašyti ir gauti iš jų informaciją, reikalingą jo funkcijoms vykdyti.

XV. BAIGIAMOSIOS NUOSTATOS

104. Darbuotojai su Taisyklėmis bei jos pakeitimais supažindinami pasirašytinai ir privalo laikytis jose nustatytų įpareigojimų bei atlikdami savo darbo funkcijas vadovautis Taisyklėse nustatytais principais. Priėmus naują darbuotoją, jis su Taisyklėmis privalo būti supažindintas pirmąją jo darbo dieną.

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

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

107. Pasikeitus asmens duomenų tvarkymą reglamentuojantiems teisės aktams, Taisyklės yra peržiūrimos ir atnaujinamos.

108. Taisyklių priedai, jeigu tokių yra, tampa neatsiejama šių Taisyklių dalimi.

Asmens duomenų
tvarkymo taisyklių
1 priedas

**MOLĖTŲ VAIKŲ SAVARANKIŠKO GYVENIMO NAMŲ NAMŲ ASMENS DUOMENŲ TVARKYMO
REGISTRAVIMO ŽURNALAS**

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

NEATITIKČIŲ REGISTRAVIMO ŽURNALAS

Eil. Nr.	Įrašo apie neatitiktį data	Neatitikties fiksavimo laikas (esant poreikiui)	Neatitikties tipas	Informaciją apie neatitiktį pateikė	Neatitikties turinys	Neatitikties identifikavimo šaltinis	Neatitikties įvertinimas	Priežastys	Korekcinis / prevencinis, koregavimo veiksmas	Už neatitikties pašalinimą atsakingi asmenys	Išsprendimo data	Faktinė sprendimo data	Neatitikties sprendimo statusas	Atlikti veiksmai, priimti sprendimai (komentarai)
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

