PATVIRTINTA
Viešosios įstaigos Ignalinos rajono
savivaldybės sveikatos centro direktoriaus
2025 m. gegužės 12 d.
įsakymu Nr. V-45

IGNAINOS RAJONO SAVIVALDYBĖS SVEIKATOS CENTRO ASMENS DUOMENŲ TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Viešosios įstaigos Ignalinos rajono savivaldybės sveikatos centro (toliau taip pat - Įstaiga) asmens duomenų tvarkymo taisyklės (toliau – Taisyklės) reguliuoja:

1.1. fizinių asmenų (toliau – Duomenų subjektas) asmens duomenų tvarkymo principus ir tikslus,
1.2. reguliuoja asmens duomenų valdytojo ir tvarkytojo funkcijas, teises bei pareigas,
1.3. nustato Duomenų subjekto teises bei jų įgyvendinimo tvarką,
1.4. įtvirtina organizacines ir technines duomenų apsaugos priemones,
1.5. reguliuoja Duomenų tvarkymą, tvarkymo veiklos įrašus,
1.6. įtvirtina asmens duomenų saugumo pažeidimų valdymą ir reagavimą į šiuos pažeidimus,
1.7. nustato poveikio asmens duomenų apsaugai vertinimą,
1.8. nustato duomenų teikimo trečiosioms šalims atvejus bei tvarką,
1.9. reguliuoja asmens duomenų gavėjus.

2. Šios Taisyklės parengtos remiantis:

2.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (toliau – ADTAĮ);

2.2. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) Nr. 2016/679 (Bendrasis duomenų apsaugos reglamentas, toliau – BDAR);

2.3. kitais duomenų apsaugą reglamentuojančiais teisės aktais.

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

Pagrindinės sąvokos:

3.1. **Asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip vardą ir pavardę, asmens identifikavimo 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.

3.2. **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. **Duomenų valdytojas –** fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones; kai tokio duomenų tvarkymo tikslai ir priemonės nustatyti Europos Sąjungos arba valstybės narės teisės, duomenų valdytojas arba konkretūs jo skyrimo kriterijai gali būti nustatyti Europos Sąjungos arba valstybės narės teise.

3.4. **Darbuotojas** – reiškia vieną ir/ ar visus Įstaigos darbuotojus.

3.5. **Duomenų tvarkytojas** - fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis.

3.6. **Duomenų gavėjas** - fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuriai atskleidžiami asmens duomenys, nesvarbu, ar tai trečioji šalis ar ne.

3.7. **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.

3.8. **Duomenų subjektas -** fizinis asmuo, kurio tapatybę galima nustatyti Asmens duomenų pagalba ir kurio asmens duomenys yra tvarkomi.

3.9. **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.

3.10. **Sveikatos duomenys** – asmens duomenys, susiję su fizine ar psichine fizinio asmens sveikata, įskaitant duomenis apie sveikatos priežiūros paslaugų teikimą, atskleidžiantys informaciją apie to fizinio asmens sveikatos būklę.

3.11. **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.

3.12. **Inspekcija** – Lietuvos Respublikos duomenų apsaugos priežiūros institucija Valstybinė duomenų apsaugos inspekcija.

3.13. **Vidaus administravimas** – veikla, kuria užtikrinamas duomenų valdytojo savarankiškas funkcionavimas (struktūros tvarkymas, personalo valdymas, turimų materialinių ir finansinių išteklių valdymas ir naudojimas, dokumentų valdymas).

4. Šios Taisyklės taikomos tvarkant Duomenų subjekto duomenis automatiniu būdu, taip pat ir neautomatiniu būdu tvarkant asmens duomenų susistemintas rinkmenas: asmens bylas, suvestines, sąrašus, registrus ir kita.

5. Šių Taisyklių reikalavimai privalomi visiems Įstaigos darbuotojams (toliau – Darbuotojai) bei kitiems asmenims, kurie tvarko Įstaigoje esančius asmens duomenis arba eidami savo pareigas juos sužino. Šių Taisyklių taip pat privalo laikytis duomenų tvarkytojai, kurie teikdami Įstaigos duomenų tvarkymo paslaugas, sužino ir tvarko asmens duomenis.

6. Duomenų valdytojas – Viešoji įstaiga Ignalinos rajono savivaldybės sveikatos centras, įstaigos kodas 195550162, adresas: Ligoninės g. 13, Ignalina.

7. Duomenų valdytojas gali tvarkyti duomenis pats arba pasitelkti duomenų tvarkytoją.

8. Už Įstaigos vykdomą duomenų tvarkymo veiklą savo kompetencijos ribose atsakingas duomenų apsaugos pareigūnas, kurio kontaktiniai duomenys skelbiami Įstaigos internetinėje svetainėje. Duomenų apsaugos pareigūno teisės, pareigos vaidmuo ir veiklos principai numatyti Duomenų apsaugos pareigūno veiklos nuostatuose, kurie yra neatskiriama šių Taisyklių dalis (Priedas Nr. 1) arba šalių sudarytoje sutartyje.

II SKYRIUS
ASMENS DUOMENŲ TVARKYMO PRINCIPAI IR TIKSLAI

9.1. Įstaigai tvarkant asmens duomenis laikomasi šių asmens duomenų tvarkymo principų:

9.1.1. asmens duomenys renkami apibrėžtais ir teisėtais tikslais ir toliau negali būti tvarkomi tikslais, nesuderinamais su nustatytaisiais prieš renkant asmens duomenis (**apibrėžtumo ir teisėtų tikslų principas**);

9.1.2. asmens duomenys tvarkomi teisėtai, sąžiningai ir skaidriai (**teisėtumo, sąžiningumo ir skaidrumo principas**);

9.1.3. asmens duomenys turi būti tikslūs ir, jei reikia, nuolat atnaujinami; netikslūs ar neišsamūs duomenys turi būti ištaisyti, papildyti, sunaikinti arba sustabdytas jų tvarkymas (**tikslumo principas**);

9.1.4. asmens duomenys turi būti tokios apimties, kuri būtina apibrėžtiems tikslams pasiekti jiems rinkti ir toliau tvarkyti, nekaupiami ir netvarkomi pertekliniai duomenys (**duomenų kiekio mažinimo principas)**;

9.1.5. asmens duomenys saugomi tokia forma, kad Duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, negu reglamentuoja teisės aktai arba tai yra būtina siekiamiems tikslams pasiekti (**saugojimo trukmės apribojimo principas**);

9.1.6. asmens duomenys 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, prieiga prie asmens duomenų suteikiama tik tiems darbuotojams, kuriems tokie duomenys yra reikalingi jų funkcijoms ir pavedimams atlikti (**vientisumo ir konfidencialumo principas**).

9.1.7. Įstaiga atsako už visų duomenų apsaugos principų laikymąsi ir savo atitikties įrodymą, asmens duomenys tvarkomi tinkamai, vedant duomenų tvarkymo įrašus (**atskaitomybės principas**).

9.2. Įstaigoje duomenų subjektų asmens duomenys tvarkomi šiais tikslais:

9.2.1. Įstaigos pacientų ir sveikatos priežiūros specialistų – sveikatos priežiūros paslaugų teikimo organizavimo bei administravimo tikslu (pacientų aptarnavimas, sveikatos priežiūros paslaugų teikimas, įskaitant nuotoliniu būdu, pacientų, sveikatos priežiūros specialistų apskaita, registravimas bei identifikavimas Privalomojo sveikatos draudimo informacinėje sistemoje „Sveidra“ (toliau „Sveidra“), ESIS, Elektroninėje sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinėje sistemoje (toliau ESPBI IS), Sodros informacinėje sistemoje, Neįgalumo ir darbingumo nustatymo tarnybos informacinėje sistemoje, Išankstinio pacientų registravimo informacinėje sistemoje (toliau – IPR), Laboratorinių tyrimų atlikimo paslaugas teikiančios įmonės vidinėje informacinėje sistemoje);

9.2.2. esamų ir buvusių darbuotojų – vidaus administravimo tikslu (esamų ir buvusių darbuotojų duomenų valdymas, darbdavio pareigų, nustatytų darbo sutartyje, teisės aktuose, tinkamas vykdymas, darbuotojų apskaitos, dokumentų, materialinių ir finansinių išteklių naudojimo, vidinės komunikacijos duomenų valdymas);

9.2.3. pretendentų į Įstaigos darbuotojus - darbuotojų atrankos vykdymo tikslu;

9.2.4. fizinių asmenų, su Įstaiga sudariusių viešojo prekių, paslaugų, darbų pirkimo, privalomos ir savanoriškos praktikos ar kitas sutartis, asmens duomenys, o juridinių asmenų – jų darbuotojų, nurodytų sutartyse, asmens duomenys - sutarčių administravimo, vykdymo ir atsiskaitymo tikslu.

9.2.5. visuomenės ir bendruomenės informavimo apie Įstaigos veiklą tikslu (informacijos apie Įstaigos veiklą, renginius, projektus, konferencijas ir pan. skelbimas Įstaigos internetiniame puslapyje, socialinių tinklų paskyrose, skelbimų lentose). Duomenų subjekto sutikimas dėl asmens duomenų tvarkymo šiuo tikslu išreiškiamas raštiškai pagal Įstaigos nustatytą formą (Taisyklių Priedas Nr. 5);

9.2.6. Įstaigos turto apsaugos tikslu;

9.2.7. Įstaigos paslaugų kokybės gerinimo tikslu;

9.3. Įstaigos tvarkomų asmens duomenų baigtinis sąrašas ir tikslai detalizuojami Įstaigos asmens duomenų tvarkymo veiklos įrašuose (Priedas Nr. 2).

III SKYRIUS
DUOMENŲ VALDYTOJAS IR TVARKYTOJAI, JŲ FUNKCIJOS, TEISĖS IR PAREIGOS

10. Duomenų valdytojas nustato asmens duomenų tvarkymo tikslus ir priemones, vykdo šiose Taisyklėse nurodytas funkcijas. Duomenų valdytojas turi šias teises:

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

10.2. paskirti už asmens duomenų apsaugą atsakingą asmenį/pareigūną;

10.3. įgalioti duomenų tvarkytojus tvarkyti asmens duomenis;

11. Duomenų valdytojas turi šias pareigas:

11.1. užtikrinti, kad būtų laikomasi ADTAĮ, BDAR ir kitų teisės aktų, reglamentuojančių asmens duomenų tvarkymą;

11.2. įgyvendinti duomenų subjekto teises ADTAĮ/ BDAR ir šiose Taisyklėse nustatyta tvarka;

11.3. užtikrinti asmens duomenų saugumą įgyvendinant technines ir organizacines asmens duomenų saugumo priemones;

11.4. tvarkyti duomenų tvarkymo veiklos įrašus;

11.5. vertinti poveikį duomenų apsaugai;

11.6. konsultuotis su Valstybine duomenų apsaugos inspekcija;

11.7. skirti duomenų apsaugos pareigūną;

11.8. pranešti apie duomenų saugumo pažeidimą;

12. Duomenų valdytojas atlieka šias funkcijas:

12.1. analizuoja technologines, metodologines ir organizacines asmens duomenų tvarkymo problemas ir priima sprendimus, reikalingus tinkamam asmens duomenų saugumo užtikrinimui;

12.2. teikia metodinę pagalbą darbuotojams ir duomenų tvarkytojams asmens duomenų tvarkymo tikslais;

12.3. organizuoja darbuotojų mokymus asmens duomenų teisinės apsaugos klausimais;

12.4. vykdo kitas funkcijas, reikalingas Duomenų valdytojo teisėms ir pareigoms įgyvendinti.

13. Duomenų tvarkytojai. Duomenų valdytojas gali įgalioti savo valdomus duomenis tvarkyti duomenų tvarkytojus, t.y. informacinių technologijų ir elektroninių ryšių paslaugų teikėjus, patarėjus, auditorius, konsultantus, saugos tarnybas, ir kitus asmenis, kurie Duomenų valdytojo valdomus duomenis tvarko Duomenų valdytojo nustatytais tikslais ir pagal jo nurodymus.

14. Prieš pasitelkiant duomenų tvarkytoją turi būti įvertintas jo patikimumas. Patikimais laikomi tokie duomenų tvarkytojai, kurie garantuoja, jog turi pakankamai ekspertinių žinių, išteklių, patikimumo tam, kad galėtų užtikrinti asmens duomenų tvarkymo saugumą.

15. Su duomenų tvarkytojais Duomenų valdytojas sudaro rašytines sutartis, kuriose numatoma, kad duomenų tvarkytojai duomenis tvarko tik pagal Duomenų valdytojo nurodymus. Šios sutartys ir jų turinys turi atitikti BDAR reikalavimus, taikomus duomenų valdytojų ir duomenų tvarkytojų sutartims dėl asmens duomenų tvarkymo. Duomenų valdytojo ir duomenų tvarkytojo sutartyje privalo būti nurodyta tvarka, kuria remiantis Įstaigos atstovui suteikiami įgaliojimai patikrinti, kaip duomenų tvarkytojas laikosi įsipareigojimų.

16. Duomenų valdytojo įgaliotų duomenų tvarkytojų sąrašas nurodomas Tvarkomų duomenų registre (Taisyklių Priedas Nr. 2). Sudarius kiekvieną naują sutartį su duomenų tvarkytoju, apie tai Įstaiga informuoja duomenų apsaugos pareigūną, kuris papildo Taisyklių Priedą Nr. 2 naujo duomenų tvarkytojo duomenimis. Atitinkamai, nutraukus sutartį su duomenų tvarkytoju, apie tai Įstaiga informuoja duomenų apsaugos pareigūną, kuris padaro atitinkamus pokyčius Tvarkomų duomenų registre (Taisyklių Priedas Nr. 2).

17. Apie visus duomenų tvarkytojų sąrašo pasikeitimus duomenų apsaugos pareigūnas informuoja Įstaigos darbuotojus, kurie savo veikloje tvarko asmens duomenis, įprastais komunikavimo būdais.

18. Duomenų tvarkytojas turi šias teises:

18.1. teikti duomenų valdytojui pasiūlymus dėl duomenų tvarkymo techninių ir programinių priemonių gerinimo;

18.2. tvarkyti asmens duomenis, kiek tam yra įgaliotas duomenų valdytojo;

19. Duomenų tvarkytojas turi šias pareigas:

19.1. įgyvendinti tinkamas organizacines ir technines duomenų saugumo priemones, skirtas asmens duomenims nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo apsaugoti;

19.2. supažindinti naujai priimtus savo darbuotojus su šiomis Taisyklėmis;

19.3. užtikrinti, kad prieiga prie asmens duomenų būtų suteikta tik Taisyklėse nustatyta tvarka įgaliotiems asmenims;

19.4. užtikrinti, kad asmens duomenys būtu saugomi Taisyklėse nustatytais terminais;

19.5. užtikrinti, kad asmens duomenys būtų tvarkomi vadovaujantis Taisyklėmis, ADTAĮ ir kitais asmens duomenų apsaugą reglamentuojančiais teisės aktais;

19.6. saugoti asmens duomenų paslaptį, neatskleisti, neperduoti tvarkomos informacijos ir nesudaryti sąlygų jokiomis priemonėmis su ja susipažinti nei vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija, tiek duomenų tvarkytojo veiklos vietoje, tiek už jos ribų;

19.7. tvarkyti duomenų tvarkymo veiklos įrašus;

19.8. padėti duomenų valdytojui užtikrinti jam numatytas pareigas;

19.9. skirti duomenų apsaugos pareigūną;

19.10. pranešti duomenų valdytojui apie duomenų saugumo pažeidimą;

20. Duomenų tvarkytojas atlieka šias funkcijas:

20.1. įgyvendina asmens duomenų saugumo priemones;

20.2. tvarko asmens duomenis pagal Duomenų valdytojo nurodymus.

IV SKYRIUS
DUOMENŲ SUBJEKTO TEISĖS IR JŲ ĮGYVENDINIMO TVARKA

21. Duomenų subjektas (įskaitant Darbuotojus), kurio duomenys tvarkomi Duomenų valdytojo veikloje, esant BDAR nustatytam pagrindui, turi šias teises:

21.1.žinoti (būti informuotam) apie savo duomenų tvarkymą (teisė žinoti);

21.2.susipažinti su savo duomenimis ir kaip jie yra tvarkomi (teisė susipažinti);

21.3.reikalauti ištaisyti arba, atsižvelgiant į asmens duomenų tvarkymo tikslus papildyti neišsamius savo asmens duomenis (teisė ištaisyti);

21.4.reikalauti ištrinti su juo susijusius asmens duomenis (teisė „būti pamirštam“);

21.5.reikalauti, kad Duomenų valdytojas apribotų asmens duomenų tvarkymą (teisė apriboti);

21.6.bet kuriuo metu nesutikti su savo asmens duomenų tvarkymu, kai toks duomenų tvarkymas vykdomas viešo intereso labui arba tvarkyti duomenis būtina siekiant teisėtų Duomenų valdytojo arba trečiosios šalies interesų (teisė nesutikti);

21.7.teisę, kad jam nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas, dėl kurio jam kyla neigiamos pasekmės ar kuris panašiu būdu daro didelį poveikį;

21.8.gauti su juo susijusius duomenis, kuriuos jis pateikė Duomenų valdytojui susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu, ir juos persiųsti kitam duomenų valdytojui (teisė į duomenų perkeliamumą);

21.9.teisę pateikti skundą Valstybinei duomenų apsaugos inspekcijai.

DUOMENŲ SUBJEKTŲ TEISIŲ ĮGYVENDINIMO TVARKA

22. Duomenų subjektas, kurio duomenys tvarkomi Duomenų valdytojo veikloje, aukščiau nurodytas savo teises gali įgyvendinti pats arba per atstovą. Jei savo teises subjektas įgyvendina per atstovą, jis privalo pateikti atstovavimo pagrindus įrodančius dokumentus.

23. Duomenų subjektas ar teisėtas jo atstovas, siekdamas įgyvendinti šiame skyriuje numatytas duomenų subjekto teises, privalo asmeniškai raštu kreiptis į Duomenų valdytoją šiame skyriuje nustatyta tvarka.

24. Jeigu dėl duomenų subjekto teisių įgyvendinimo kreipiamasi raštu asmeniškai, duomenų subjektas turi patvirtinti savo tapatybę pateikdamas asmens tapatybę patvirtinantį dokumentą. To nepadarius, duomenų subjekto teisės nėra įgyvendinamos.

25. Jeigu dėl duomenų subjekto teisių įgyvendinimo kreipiamasi raštu, pateikiant prašymą paštu, tuomet kartu su prašymu turi būti pateikta notaro ar kito tinkamai įgalioto asmens patvirtinta asmens tapatybę patvirtinančio dokumento kopija, ar kiti dokumentai (informacija) leidžiantys Įstaigai identifikuoti prašymą pateikusį asmenį. Teikiant prašymą elektroninėmis priemonėmis, prašymas turi būti pasirašytas kvalifikuotu elektroniniu parašu arba jis turi būti suformuotas elektroninėmis priemonėmis, kurios leidžia užtikrinti teksto vientisumą ir nepakeičiamumą.

26. Esant abejonių dėl duomenų subjekto tapatybės, Duomenų valdytojas prašo papildomos informacijos, reikalingos ja įsitikinti.

27. Prašymas įgyvendinti duomenų subjekto teises turi būti įskaitomas, asmens (duomenų subjekto ar jo teisėto atstovo) pasirašytas, jame turi būti nurodyti duomenų subjekto vardas, pavardė, adresas ir (ar) kiti kontaktiniai duomenys ryšiui palaikyti ar kuriais pageidaujama gauti atsakymą dėl duomenų subjekto teisių įgyvendinimo. Jei prašyme nenurodoma kokiu būdu pageidaujama gauti atsakymą, tai jis pateikiamas tokiu būdu kokiu buvo prašoma pateikti informaciją.

28. Visais klausimais, susijusiais su duomenų subjekto asmens duomenų tvarkymu ir naudojimusi savo teisėmis, duomenų subjektas turi teisę kreiptis į Įstaigos duomenų apsaugos pareigūną. Siekiant užtikrinti BDAR 38 straipsnio 5 dalyje įtvirtintą konfidencialumą, kreipiantis į Įstaigos duomenų apsaugos pareigūną paštu, ant voko užrašoma, kad korespondencija skirta duomenų apsaugos pareigūnui.

29. Jeigu prašymas pateiktas nesilaikant šiose taisyklėse nustatytos tvarkos ir reikalavimų, ar subjekto prašymas akivaizdžiai nepagrįstas ar neproporcingas, visų pirma dėl jų pasikartojančio turinio, jis nenagrinėjamas, ir nedelsiant, bet ne vėliau kaip per 3 darbo dienas, asmuo pateikęs prašymą apie tai informuojamas nurodant priežastis. Duomenų valdytojas turi gebėti įrodyti, kad prašymas yra akivaizdžiai nepagrįstas arba neproporcingas.

30. Gavus duomenų subjekto prašymą įgyvendinti teises, ne vėliau kaip per vieną mėnesį nuo prašymo gavimo, jam pateikiama informacija apie tai, kokių veiksmų buvo imtasi pagal gautą prašymą. Jeigu bus vėluojama pateikti informaciją, per nurodytą terminą pateikiama informacija, nurodant vėlavimo priežastis ir apie galimybę pateikti skundą Valstybinei duomenų apsaugos inspekcijai.

31. Jeigu prašymo nagrinėjimo metu nustatoma, jog duomenų subjekto teisės yra apribotos BDAR 23 straipsnio 1 dalyje numatytais pagrindais, duomenų subjektas apie tai informuojamas.

32. Įstaigos veiksmus ar neveikimą įgyvendinant duomenų subjekto teises duomenų subjektas turi teisę skųsti pats arba duomenų subjekto atstovas, taip pat jo įgaliota ne pelno įstaiga, organizacija ar asociacija, atitinkanti BDAR 80 straipsnio reikalavimus, Valstybinei duomenų apsaugos inspekcijai. Už visų šiose Taisyklėse nurodytų duomenų subjekto teisių įgyvendinimą atsakingas duomenų apsaugos pareigūnas ir visi Duomenų valdytojo darbuotojai jų kompetencijos ribose.

33. Jei duomenų subjekto, pateikusio pagrįstą prašymą dėl savo teisių įgyvendinimo, asmens duomenis Duomenų valdytojo vardu tvarko duomenų tvarkytojai, Duomenų valdytojas kreipiasi į juos ir informuoja apie duomenų subjekto prašymą. Duomenų valdytojas kontroliuoja, kad duomenų tvarkytojai kaip įmanoma greičiau padėtų Duomenų valdytojui įgyvendinti duomenų subjekto teises ir informuotų Duomenų valdytoją, kad duomenų subjekto teisės duomenų tvarkytojo tvarkomų asmens duomenų apimtyje yra įgyvendintos.

34. Jei kurių nors duomenų subjekto teisių įgyvendinimo aspektų nereglamentuoja Taisyklės ir kiti asmens duomenų apsaugos teisės aktai, taikomos Prašymų ir skundų nagrinėjimo ir asmenų aptarnavimo viešojo administravimo subjektuose taisyklės, patvirtintos Lietuvos Respublikos Vyriausybės 2007 m. rugpjūčio 22 d.

nutarimu Nr. 875 „Dėl Prašymų ir skundų nagrinėjimo ir asmenų aptarnavimo viešojo administravimo subjektuose taisyklių patvirtinimo“.

V SKYRIUS
ORGANIZACINĖS IR TECHNINĖS ASMENS DUOMENŲ APSAUGOS PRIEMONĖS

35. Siekiant apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, nuo bet kokio kito neteisėto tvarkymo Įstaigos darbuotojai bei Duomenų tvarkytojai turi taikyti atitinkamas administracines ir technines priemones.

36. Įstaigoje darbuotojai bei Duomenų tvarkytojai taiko tokias priemones:

36.1. saugus ir tinkamas techninės įrangos išdėstymas ir priežiūra, informacinių sistemų priežiūra, tinklo (LAN, belaidžio) valdymas, naudojimosi internetu saugumo užtikrinimas ir kitos informacinių technologijų priemonės, už kurių įgyvendinimą ir priežiūrą atsako Įstaigos direktoriaus įsakymu paskirtas Įstaigos informacinių sistemų specialistas

36.2. griežtas priešgaisrinės apsaugos tarnybos nustatytų normų laikymasis;

36.3. prieiga prie asmens duomenų bei teisė atlikti duomenų tvarkymo veiksmus suteikiama tik tiems Įstaigos darbuotojams ar Duomenų tvarkytojams, kuriems tokia prieiga reikalinga pagal užimamas pareigas bei siekiant atlikti darbines funkcijas. Darbo santykiams pasibaigus, darbuotojui prieigos prie informacinių sistemų, registrų ir kitų programų teisės nedelsiant panaikinamos;

36.4. **Darbuotojai ir/ar Duomenų tvarkytojai prieigai prie kompiuterių bei informacinių sistemų naudoja unikalius slaptažodžius taip pat ekrano užsklandas su slaptažodžiais**;

36.5. Užtikrinama asmens duomenų apsauga nuo neteisėtų prisijungimo prie vidinio kompiuterinio tinklo elektroninių ryšių priemonėmis;

36.6. Užtikrinama asmens duomenų, esančių išorinėse duomenų laikmenose ir elektroniniame pašte, saugos kontrolė;

36.7. užtikrinamas neaktualių Duomenų tinkamas sunaikinimas;

36.8. Įstaigos darbuotojai turi laikytis konfidencialumo principo ir laikyti paslaptyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jie susipažino eidami savo pareigas, nebent tokia informacija būtų vieša pagal galiojančių įstatymų ar kitų teisės aktų nuostatas. Konfidencialumui ir asmens duomenų saugumui užtikrinti Įstaigos darbuotojai pasirašo konfidencialumo pasižadėjimą, kurio forma yra šių Taisyklių Priedas Nr. 4.;

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

36.10. Įstaigos informacinėse sistemose ir kompiuterių tinkluose įgyvendinamos šios saugumo priemonės:

36.10.1. **periodiškai, ne rečiau nei kas tris mėnesius pakeičiami prisijungimų prie kompiuterių bei informacinių sistemų, kuriose yra saugomi asmens duomenų įrašai, slaptažodžiai. Slaptažodžiai taip pat keičiami ne pagal grafiką esant būtinybei (pasikeitus darbuotojui, iškilus įsilaužimo grėsmei ir pan.).**

36.10.2. šifruojami elektroniniu paštu perduodami asmens duomenys;

36.10.3. fiksuojami prisijungimų prie asmens duomenų įrašai: bylos, prie kurių buvo jungtasi, atlikti veiksmai su asmens duomenimis (įvedimas, peržiūra, keitimas, naikinimas ir kiti asmens duomenų tvarkymo veiksmai). Šie įrašai turi būti saugomi ne trumpiau kaip 1 metus;

36.10.4. kitos organizacinės bei techninės saugumo priemonės, numatytos patvirtintuose Įstaigos informacinės sistemos duomenų saugos nuostatuose.

36.11. Įstaigos Direktoriaus įsakymu paskiriamas Įstaigos informacinių sistemų specialistas, kuris tuo pačiu negali būti ir asmens duomenų apsaugos pareigūnu;

VI SKYRIUS
DUOMENŲ TVARKYMAS. TVARKYMO VEIKLOS ĮRAŠAI

37. Duomenys saugomi Taisyklių priede Nr. 2 nurodytose informacinėse sistemose, taip pat programose, darbuotojų kompiuteriuose, registratūroje, archyve, rakinamose spintose.

38 Duomenys Įstaigoje renkami teisės aktų nustatyta tvarka, juos gaunant tiesiogiai iš duomenų subjekto, iš kitų informacinių sistemų, kurių duomenis Įstaiga turi teisę gauti, oficialiai užklausiant reikalingą informaciją tvarkančių ir turinčių teisę ją teikti subjektų ar sutarčių pagrindu. Esant būtinybei, asmens duomenys tvarkomi gaunant duomenų subjekto sutikimą.

39. Duomenų tvarkymo funkcijas vykdantys darbuotojai, siekdami užkirsti kelią atsitiktiniam ar neteisėtam asmens duomenų sunaikinimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam tvarkymui, turi saugoti dokumentus bei duomenų rinkmenas tinkamai ir saugiai bei vengti nereikalingų kopijų darymo. Dokumentų kopijos, kuriose nurodomi asmens duomenys, turi būti sunaikintos taip, kad šių dokumentų nebūtų galima atkurti ir atpažinti jų turinio.

40. Darbuotojai, kurių kompiuteriuose saugomi duomenys arba iš kurių kompiuterių galima patekti į vietinio tinklo sritis, kuriose yra saugomi duomenys, arba informacines sistemas, kuriose yra asmens duomenys, privalo naudoti slaptažodžius. Slaptažodžiai turi būti keičiami periodiškai ne rečiau kaip vieną kartą per tris mėnesius, taip pat kitais atvejais, susidarius tam tikroms aplinkybėms (pasikeitus darbuotojui, iškilus įsilaužimo grėsmei, kilus įtarimui, kad slaptažodis tapo žinomas tretiesiems asmenims, ir pan.).

41. Už kompiuterių priežiūrą atsakingas darbuotojas/įmonė užtikrina, kad asmens duomenų rinkmenos nebūtų matomos iš kitų kompiuterių, o antivirusinės programos atnaujinamos periodiškai.

42. Pasibaigus šiose Taisyklėse nurodytiems Įstaigos tvarkomų asmens duomenų saugojimo terminams, asmens duomenys, kurie buvo užfiksuoti ir saugojami kompiuterinėje įrangoje ar duomenų laikmenose (USB, CD, DVD diskai, magnetiniai diskeliai ir juostos), turi būti sunaikinami.

Duomenų tvarkymo veiklos įrašai

43. Įstaigoje daromi šie duomenų tvarkymo veiklos įrašai:

43.1. tvarkomų duomenų registras, kuriame numatyti duomenų tvarkymo tikslai, pagrindas, duomenų subjektų kategorijos, tvarkomų duomenų sąrašas ir saugojimo terminai, duomenų tvarkytojų ir gavėjų sąrašas bei darbuotojų, kuriems suteikiama teisė tvarkyti asmens duomenis sąrašas (Priedas Nr. 2)

43.2. vienkartinių duomenų tvarkymo veiklos atvejų sąrašas (Priedas Nr. 2)

43.3. asmens duomenų incidentų registras (Priedas Nr. 3)

44. Duomenų tvarkymo veiklos įrašus pildo duomenų apsaugos pareigūnas.

45. Duomenų tvarkymo veiklos įrašai yra saugomi Įstaigoje arba pas Duomenų apsaugos pareigūną.

46. Įgaliotai valdžios institucijai pateikus pagrįstą reikalavimą susipažinti su duomenų tvarkymo veiklos įrašais, atitinkamus įrašus per prašyme nustatytą terminą pateikia Įstaigos direktorius arba, jo pavedimu, kitas Įstaigos darbuotojas.

47. Įrašai yra saugomi tokiu formatu ir tokia tvarka, kad pareikalavus Valstybinei duomenų apsaugos inspekcijai būtų galima perduoti reikalaujamus įrašus.

48. Duomenų tvarkymo veiklos įrašuose esanti informacija yra patikrinama ir atnaujinama ne rečiau kaip 2 (du) kartus per kalendorinius metus.

49. Už duomenų tvarkymo veiklos įrašų patikrinimą ir informacijos atnaujinimą yra atsakingas duomenų apsaugos pareigūnas.

50. Netaikoma.

VII SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO IR REAGAVIMO Į ŠIUOS PAŽEIDIMUS TVARKA

51. Įstaigos darbuotojai, turintys prieigos prie asmens duomenų teisę, pastebėję duomenų saugumo pažeidimus (veiksmus ar neveikimą, galinčius sukelti ar sukeliančius grėsmę asmens duomenų saugumui), turi **per 2 valandas nuo galimo duomenų saugumo pažeidimo pastebėjimo** informuoti duomenų apsaugos pareigūną, kurio kontaktai nurodyti Įstaigos tinklapyje, taip pat Įstaigos vadovą.

52. Duomenų valdytojas užtikrina tinkamą asmens duomenų pažeidimo incidentų stebėjimą, nustatymą bei įvertinimą.

53. Duomenų pažeidimo incidentu laikomas įvykis, kuris sukelia arba gali sukelti, be kita ko:

53.1. asmens duomenų paviešinimą;

53.2. asmens duomenų nutekėjimą, t. y. kai asmens duomenys tampa prieinami asmenims, kurie neturi teisės jų tvarkyti;

53.3. asmens duomenų tvarkymui naudojamos įrangos gedimus, kurie gali nulemti asmens duomenų sunaikinimą;

53.4. asmens duomenų klaidas.

54. Kiekvienas Įstaigos darbuotojas, kuris pastebėjo duomenų pažeidimo incidentą, privalo nedelsdamas, tačiau ne vėliau kaip per 2 darbo valandas, apie tai raštu ar elektroninėmis priemonėmis informuoti duomenų apsaugos pareigūną bei Įstaigos vadovą. Darbuotojo pareiga pranešti apie duomenų pažeidimo incidentą turi pirmenybę prieš visus kitus Įstaigos darbuotojo darbus, o darbuotojo delsimas pateikti tokį

pranešimą arba jo nepateikimas negali būti pateisinamas jokiomis priežastimis, įskaitant, bet neapsiribojant, svarbesnių darbų atlikimu, vadovų nebuvimu, atostogomis ar kitomis priežastimis.

54[1]. Duomenų tvarkytojai, sužinoję apie asmens duomenų saugumo pažeidimą, nedelsdami, ne vėliau kaip per 1 darbo dieną, apie tai raštu praneša duomenų apsaugos pareigūnui, pateikdami informaciją, numatytą Reglamento (ES) 2016/679 33 straipsnio 3 dalyje. Duomenų tvarkytojai pateikia duomenų apsaugos pareigūnui jo prašomą informaciją, susijusią su Pažeidimu ir jo tyrimu, per duomenų apsaugos pareigūno nurodytą terminą. Duomenų tvarkytojų pareigos, susijusios su pranešimu apie duomenų saugumo pažeidimą Įstaigai bei su bendradarbiavimu tiriant pažeidimą, įtvirtinamos su duomenų tvarkytoju sudaromoje sutartyje.

55. Atlikęs pirminį duomenų pažeidimo incidento įvertinimą, duomenų apsaugos pareigūnas:

55.1. nedelsdamas nagrinėja pranešime nurodytas aplinkybes, atlieka galimai padaryto asmens duomenų saugumo pažeidimo tyrimą;

55.2. įvertina, ar padarytas asmens duomenų saugumo pažeidimas;

55.3. jei asmens duomenų saugumo pažeidimas padarytas, nustato, kokio tipo pažeidimas padarytas, asmens duomenų kategorijas, įskaitant specialių kategorijų asmens duomenis, kurios buvo susijusios su pažeidimu, pažeidimo priežastis, lėmusias asmens duomenų saugumo pažeidimą, apimtį (duomenų subjektų kategorijos ir skaičius), žalą, padarytą asmeniui;

55.3[1]. Pažeidimo tyrimo metu nustatomas Pažeidimo tipas. Galimi Pažeidimo tipai:

55.3[1].1. Konfidencialumo pažeidimas – kai be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;

55.3[1].2. Prieinamumo pažeidimas – kai netyčia arba neteisėtai prarandama prieiga prie asmens duomenų arba asmens duomenys sunaikinami;

55.3[1].3. Vientisumo pažeidimas – kai asmens duomenys pakeičiami be leidimo ar netyčia.

55.4. pasitelkia darbuotojus (informacinių technologijų specialistus ir pan.) ir duomenų tvarkytojo darbuotojus, jei tai būtina;

55.5. nustato, kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas asmens duomenų saugumo pažeidimas (pvz., naudoti atsargines kopijas, kad būtų atkurti prarasti ar sugadinti duomenys ar kt.);

55.6. nustato, ar būtina nedelsiant pranešti duomenų subjektui apie asmens duomenų saugumo pažeidimą.;

55.7. sprendžia dėl pranešimo apie incidentą Valstybinei duomenų apsaugos inspekcijai poreikio (pranešti nereikia, jei įvykęs pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms);

55.8. nustatęs, kad duomenų saugumo pažeidimas gali sukelti didelį pavojų fizinių asmenų teisėms ir laisvėms, todėl apie jį pranešti Inspekcijai būtina, užtikrina, kad apie pažeidimą Inspekcijai būtų pranešta ne vėliau kaip per 72 val. nuo sužinojimo apie duomenų saugumo pažeidimą momento. Pranešime turi būti nurodoma bent:

55.8.1. duomenų saugumo pažeidimo pobūdis (įskaitant, jei įmanoma, atitinkamų duomenų subjektų kategorijas ir apytikslį skaičių), galimos jo pasekmės,

55.8.2. duomenų apsaugos pareigūno kontaktiniai duomenys,

55.8.3. atlikti ar planuojami atlikti veiksmai, kaip pašalinti duomenų saugumo pažeidimą ar galimą neigiamą jo poveikį ir pasekmes (pvz. tam tikrų el. pašto adresų siunčiamų laiškų blokavimas ir pan. veiksmai),

55.9. įvertina, ar dėl šio asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinio asmens teisėms ir laisvėms ir ar turi būti informuojami duomenų subjektai, kurių duomenys buvo pažeisti;

55.10. jei nustatoma, kad dėl duomenų saugumo pažeidimo duomenų subjektų teisėms ir laisvėms gali kilti didelis pavojus, todėl pranešti duomenų subjektams būtina, inicijuoja kuo skubesnį duomenų subjektų, kurių duomenys buvo pažeisti, informavimą (išskyrus BDAR numatytus atvejus, kuomet apie pažeidimą duomenų subjektams pranešti nereikia ar leidžiama apie jį paskelbti viešai). Tokiu atveju Įstaigos duomenų apsaugos pareigūnas ar kitas įgaliotas asmuo parengia pranešimą bei nepagrįstai nedelsdamas informuoja kiekvieną asmens duomenų subjektą, kurio asmens duomenys paveikti, apie duomenų pažeidimo incidentą, kad jis galėtų imtis reikiamų priemonių užkirsti tam kelią. Pranešime turi būti pateikti bent:

55.10.1. duomenų apsaugos pareigūno kontaktiniai duomenys,

55.10.2. aprašytas duomenų saugumo pažeidimo pobūdis bei galimos jo pasekmės,

55.10.3. pateiktos atitinkamam fiziniam asmeniui skirtos rekomendacijos, kaip pašalinti duomenų saugumo pažeidimą ar galimą neigiamą jo poveikį ir pasekmes (pvz. tam tikrų el. pašto adresų siunčiamų laiškų blokavimas ir pan. veiksmai);

55.11. jeigu reikia, nedelsdamas kreipiasi į trečiasis šalis, kurios gali padėti suvaldyti duomenų pažeidimo incidento padarinius.

56. Apie kiekvieną su asmens duomenimis susijusį incidentą privalo būti pranešta Įstaigos vadovui, taip pat kiekvienas toks incidentas privalo būti užregistruotas Asmens duomenų incidentų registre (Taisyklių Priedas Nr. 3). Už Asmens duomenų incidentų registro pildymą atsako duomenų apsaugos pareigūnas.

VIII SKYRIUS
POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

57. Įstaiga tam tikrais atvejais, įskaitant, bet neapsiribojant, prieš pradedant tvarkyti duomenis naujais būdais, privalo atlikti poveikio duomenų apsaugai vertinimą. Poveikio duomenų apsaugai vertinimas turi būti atliekamas Inspekcijos direktoriaus įsakymu patvirtiname Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąraše numatytais atvejais, tame tarpe, jei Duomenų tvarkymas:

57.1. 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 specialių kategorijų duomenys tokie kaip sveikata, būtų pradėti naudoti nauji technologiniai sprendimai, pavyzdžiui, veido atpažinimo sistemos, kt.);

57.2. 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;

57.3. būtų pradėtas vykdyti sistemingas vaizdo stebėjimas dideliu mastu;

57.4. būtų pradėti tvarkyti specialių kategorijų Asmens duomenys dideliu mastu.

58. Jei Įstaiga, atlikdamas poveikio duomenų apsaugai vertinimą, nustatytų, kad Duomenų subjektų teisėms ir laisvėms gali kilti didelis pavojus, jis privalo konsultuotis su Valstybine duomenų apsaugos inspekcija dėl tinkamų saugumo ir kitų priemonių įgyvendinimo.

59. Atliekant poveikio duomenų apsaugai vertinimą, Įstaiga privalo nustatyti:

59.1. kokia bus atliekama duomenų tvarkymo operacija (-os);

59.2. kiek konkreti duomenų tvarkymo operacija yra reikalinga ir proporcinga;

59.3. koks gali būti poveikis Duomenų subjektams;

59.4. Kokios yra galimos potencialių pavojų šalinimo, saugumo užtikrinimo priemonės.

60. Įstaiga privalo užtikrinti, kad šiame skyriuje aprašytais ir Įstaigos dokumentuose numatytais atvejais atliekamas poveikio duomenų apsaugai vertinimas, būtų tinkamai dokumentuotas ir saugomas.

61. Poveikio duomenų apsaugai vertinimas gali būti atliekamas ir esamoms duomenų tvarkymo operacijoms (t.y. vykdomoms iki BDAR įsigaliojimo), jei tose operacijose atsirastų reikšmingų pokyčių, pavyzdžiui, būtų pradėtos naudoti naujos technologijos, duomenys būtų pradėti tvarkyti kitu tikslu nei iki tol, atsirastų naujos rizikos, susijusios su įvykdytomis kibernetinėmis atakomis, įsilaužimais į Įstaigos sistemas, duomenys būtų pradėti teikti naujiems duomenų gavėjams, tvarkytojams už ES ribų, kt.

62. Poveikio duomenų apsaugai vertinimas taip pat gali būti atliekamas ir šiame skyriuje neaptartais atvejais, bet esant Įstaigos vadovo, duomenų apsaugos pareigūno ar Inspekcijos rekomendacijai tai atlikti.

IX SKYRIUS
ASMENS DUOMENŲ TEIKIMAS TREČIOSIOMS ŠALIMS

63. Duomenų teikimas trečiosioms šalims:

63.1. į neįgaliotų trečiųjų šalių elektroninius ar kitokia forma (išskyrus telefonu) pateiktus prašymus suteikti jiems informaciją apie Duomenų subjektus turi būti atsakoma tik jeigu galima identifikuoti Rašytinį prašymą pateikusį (pasirašiusį) asmenį, 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 Įstaigoje tvarkomus asmens duomenis telefonu neteikiama.**

63.2. Vienkartinio duomenų teikimo atveju Įstaiga, teikdama asmens duomenis pagal duomenų gavėjo rašytinį prašymą**, prioritetą teikia duomenų teikimui elektroninių ryšių priemonėmis**.

64. Konfidencialumo reikalavimas netaikomas ir informacija (asmens duomenys) gali būti suteikta tik tarnybiniais tikslais, neturint raštiško Duomenų subjekto sutikimo:

64.1. Valstybės vaiko teisių apsaugos ir įvaikinimo tarnybai ar jos įgaliotam teritoriniam skyriui ir/ar policijai įtarus galimą vaiko teisių pažeidimą LR Vaiko teisių apsaugos pagrindų įstatyme numatyta tvarka bei atvejais;

64.2. mokesčių administratoriams, teismui, prokuratūrai, ikiteisminio tyrimo įstaigoms bei kitoms institucijoms, kurioms tokį teisinį pagrindą suteikia Lietuvos Respublikos įstatymai.

65. 64 punkte išvardytos institucijos ar įstaigos pateikia vadovo arba jo įgalioto asmens pasirašytą prašymą, pavedimą, sprendimą ar kitą dokumentą, kurį tokiais atvejais reikia pateikti pagal tų institucijų ar įstaigų darbą reglamentuojančius teisės aktus.

66. Vadovaudamasi Lietuvos Respublikos įstatymais ir kitais teisės aktais, Įstaiga informaciją (Asmens duomenis) apie Duomenų subjektą pateikia savo iniciatyva (nesant Duomenų subjekto ar Trečiosios šalies Rašytinio prašymo) ir be Duomenų subjekto sutikimo šiais atvejais:

66.1. kai reikia pranešti apie įtariamą nusikalstamą veiką;

66.2. Valstybės vaiko teisių apsaugos ir įvaikinimo tarnybai ar jos įgaliotam teritoriniam skyriui ir/ar policijai įtarus galimą vaiko teisių pažeidimą LR Vaiko teisių apsaugos pagrindų įstatyme numatyta tvarka bei atvejais.

X SKYRIUS
DUOMENŲ GAVĖJAI

67. Duomenų valdytojo valdomi asmens duomenys tretiesiems asmenims teikiami esant duomenų subjekto sutikimui arba kitam teisėtam duomenų teikimo pagrindui.

68. Apie prašymus teikti asmens duomenis (vienkartinius ir daugkartinius) yra informuojamas duomenų apsaugos pareigūnas iki duomenų teikimo pradžios arba atsisakymo teikti duomenis išsiuntimo.

69. Vienkartinio ir daugkartinio duomenų teikimo atvejais apie teisinio pagrindo Įstaigos valdomų duomenų teikimui buvimą sprendimą priima duomenų apsaugos pareigūnas.

70. Nesant teisinio pagrindo teikti Įstaigos valdomus duomenis, apie tai informuojamas duomenų prašantis asmuo/institucija. Apie atsisakymą teikti duomenis padaromas įrašas Vienkartinių duomenų tvarkymo veiklos atvejų sąraše (Taisyklių Priedas Nr. 2). Už įrašo padarymą atsakingas duomenų apsaugos pareigūnas.

71. Įstaigos tvarkomų asmens duomenų gavėjais gali būti fiziniai ar juridiniai asmenys, pateikę Įstaigai prašymą dėl vienkartinio duomenų teikimo ar su kuriais pasirašytos duomenų teikimo sutartys, taip pat kiti juridiniai asmenys, kuriems asmens duomenys teikiami Įstaigos teisėtų interesų užtikrinimo tikslais ar kitu teisiniu pagrindu (teisėsaugos ir teisėtvarkos institucijoms, teismams, antstoliams, advokatams ir kt.).

72. Įstaigos darbuotojų asmens duomenys gali būti teikiami valstybės, savivaldybės institucijoms, kurios LR įstatymų nustatyta tvarka įgaliotos tvarkyti asmens duomenis (periodinis duomenų teikimas Socialinio draudimo fondo valdybai (SODRAI), Valstybinei mokesčių inspekcijai prie Finansų ministerijos, Karo prievolės administravimo tarnybos teritoriniam skyriui ir kt.). Įstaigos darbuotojų duomenys taip pat gali būti teikiami tretiesiems asmenims pasirašytų sutarčių pagrindu, pavyzdžiui, siekiant užsakyti Įstaigos darbuotojams kelionės bilietus jų komandiruočių metu ir kt.

73. Įstaigos valdomi duomenys duomenų gavėjams už Europos ekonominės erdvės ribų teikiami tik užtikrinus tinkamą duomenų teisinės apsaugos lygį (pvz., remiantis ES standartinėmis sutarčių sąlygomis, „Privacy Shield“ sistema, Europos Komisijos sprendimais dėl adekvačios duomenų apsaugos ar kt.) arba, jeigu nėra kito pagrindo, gavus Valstybinės duomenų apsaugos inspekcijos leidimą.

74. Duomenų valdytojo tvarkomų asmens duomenų gavėjų sąrašas pateikiamas Tvarkomų duomenų registre (Taisyklių Priedas Nr. 2).

XI SKYRIUS
DUOMENŲ SAUGOJIMO TERMINAI

75. Įstaiga taiko skirtingus Asmens duomenų saugojimo terminus priklausomai nuo tvarkomų Asmens duomenų kategorijų. Dokumentai, sudaryti vykdant vidaus administravimo funkcijas, saugomi Lietuvos vyriausiojo archyvaro tvirtinamoje Bendrųjų dokumentų saugojimo terminų rodyklėje ir kituose norminiuose teisės aktuose nustatytą laiką. Dokumentai, sudaryti teikiant sveikatos priežiūros paslaugas saugomi, be kita ko, vadovaujantis LR Sveikatos apsaugos ministro 1999-11-29 įsakymu Nr. 515 (aktualia redakcija) patvirtintais privalomų sveikatos statistikos apskaitos ir kitų formų, pildomų sveikatos priežiūros įstaigose, saugojimo terminais. Jei teisės aktais nenurodyta kitaip, taikomi šie Asmens duomenų saugojimo terminai:

Eil. Nr.	Asmens duomenų kategorija	Saugojimo terminas
1	Darbuotojų duomenys susiję su darbo santykiais	50 metų po darbo sutarties nutraukimo arba kitą minimalų terminą, kurį nustato Bendrųjų

		dokumentų saugojimo terminų rodyklė, patvirtinta Lietuvos vyriausiojo archyvaro įsakymu.
2	Kandidatų į darbą pateikti duomenys	3 metai nuo paskutinio duomenų gavimo
3	Pacientų gydymo stacionare ligos istorija/ kortelė	25 metai
4	Pacientų ambulatorinė asmens sveikatos istorija	15 metų nustojus lankytis pacientui
5	Fizinių asmenų, su Įstaiga sudariusių viešojo prekių, paslaugų, darbų pirkimo, privalomos ir savanoriškos praktikos ar kitas sutartis, asmens duomenys, o juridinių asmenų – jų darbuotojų, nurodytų sutartyse, asmens duomenys	10 metų po sutarčių pasibaigimo
6	Įstaigos vadovo įsakymai	10 metų
7	Savivaldos institucijų veiklos dokumentai (protokolai, kiti dokumentai)	5 metai
8	Valstybės ir savivaldybės biudžeto lėšomis finansuojamų projektų vykdymo dokumentai	5 metai (po projekto įgyvendinimo)

76. Duomenys, reikalingi siekiant pareikšti, vykdyti arba apginti Įstaigos teises bei pareigas saugomi tiek, kiek yra būtina tokiems tikslams pasiekti neteismine ar teismine tvarka.

XII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

77. Darbuotojai, kurie yra įgalioti tvarkyti asmens duomenis arba eidami savo pareigas juos sužino, privalo laikytis šių Taisyklių, pagrindinių asmens duomenų tvarkymo reikalavimų bei konfidencialumo ir saugumo reikalavimų, įtvirtintų BDAR, ADTAĮ ir šiose Taisyklėse. Darbuotojai pažeidę Taisykles ir (ar) ADTAĮ/ BDAR atsako teisės aktų nustatyta tvarka.

78. Patvirtinus Taisykles, **darbuotojai su jomis supažindinami pasirašytinai**. Priėmus naują darbuotoją, jis su Taisyklėmis privalo būti supažindintas per pirmąsias tris darbo dienas. Už supažindinimą su Taisyklėmis Įstaigoje atsakingas Įstaigos sekretorius/administratorius.

79. Įstaiga užtikrina darbuotojų, kuriems suteikta teisė tvarkyti asmens duomenis, mokymus.

80. Už Taisyklių nuostatų laikymosi priežiūrą atsakingas Įstaigos direktoriaus įsakymu paskirtas duomenų apsaugos pareigūnas, kuris, įvertinęs Taisyklių taikymo praktiką, esant poreikiui, inicijuoja Taisyklių atnaujinimą.

81. Šias Taisykles pažeidę asmenys atsako Lietuvos Respublikos teisės aktu nustatyta tvarka.

82. Taisyklės įsigalioja jas patvirtinus. Taisyklės, jų pakeitimai ar papildymai skelbiami Įstaigos interneto svetainėje.

83. Taisyklės peržiūrimos ir, reikalui esant, atnaujinamos pasikeitus asmens duomenų apsaugą reglamentuojantiems teisės aktams, bet ne rečiau kaip kartą per dvejus metus.