PATVIRTINTA
Vilniaus lopšelio–darželio „Varpelis“
Direktoriaus
2025 m. spalio 3 d. įsakymu Nr. V-83

VILNIAUS LOPŠELIO–DARŽELIO „VARPELIS“ ASMENS DUOMENŲ TVARKYMO TAISYKLĖS

Vilnius
2025

I. SKYRIUS
BENDROSIOS NUOSTATOS IR TAIKYMO SRITIS

1. Šios asmens duomenų tvarkymo taisyklės (toliau – Taisyklės) nustato Vilniaus lopšelio-darželio „Varpelis“ (toliau – Įstaiga) įgyvendinamus asmens duomenų tvarkymo principus, organizacines ir technines priemones, siekiant užtikrinti tinkamą duomenų subjektų asmens duomenų apsaugą.

2. Taisyklės taikomos:

- darbuotojų ir kandidatų į darbo vietas duomenims;
- praktikantų ir savanorių duomenims;
- ugdytinių ir jų tėvų (globėjų) duomenims, kartu su ugdytinių duomenų tvarkymo taisyklėmis;
- tretiesiems asmenims, kai jų duomenys tvarkomi Įstaigos veikloje.

3. Šios taisyklės parengtos vadovaujantis:

- 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 (BDAR);
- Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (ADTAĮ);
- kitais Lietuvos Respublikos ir ES teisės aktais.

4. Šios Taisyklės taip pat apibrėžia duomenų subjektų teisių įgyvendinimo tvarką, Duomenų valdytojo, duomenų tvarkytojo teises, pareigas ir atsakomybę.

5. Šių Taisyklių privalo laikytis visi Įstaigos darbuotojai bei kiti asmenys, gaunantys prieigą prie Įstaigos tvarkomų duomenų.

II. SKYRIUS
NAUDOJAMOS SĄVOKOS

6. Šiose taisyklėse vartojamos sąvokos suprantamos taip, kaip apibrėžta BDAR ir nacionaliniuose teisės aktuose:

- **Asmens duomenys –** bet kuri informacija apie fizinį asmenį, kurio tapatybė yra žinoma arba gali būti nustatyta.
- **Duomenų subjektas** – fizinis asmuo, kurio duomenys yra renkami, saugomi ar kitaip naudojami.
- **Duomenų valdytojas** – kompetentinga institucija, kuri viena ar kartu su kitais nustato asmens duomenų tvarkymo tikslus ir priemones; kai tokio duomenų tvarkymo tikslai ir priemonės nustatyti Sąjungos arba valstybės narės teisės, duomenų valdytojas arba konkretūs jo skyrimo kriterijai gali būti nustatyti Sąjungos arba valstybės narės teise.
- **Duomenų tvarkytojas** – fizinis ar juridinis asmuo, kuris tvarko duomenis Duomenų valdytojo vardu.
- **Duomenų apsaugos pareigūnas** – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kurie duomenų valdytojo vardu tvarko asmens duomenis.
- **Sutikimas** – aiškus duomenų subjekto patvirtinimas, kad jo duomenys gali būti tvarkomi.
- **Poveikio duomenų apsaugai vertinimas (PDAV)** – procesas, skirtas įvertinti duomenų tvarkymo rizikas asmenų teisėms ir laisvėms.

7. Kitos šiose Taisyklėse vartojamos sąvokos Reglamente ir kituose Lietuvos Respublikos teisės aktuose apibrėžtą traktuotę.

III. SKYRIUS
TVARKYMO PRINCIPAI

8. Tvarkant duomenis Įstaigoje laikomasi šių principų:

- Teisėtumo, sąžiningumo ir skaidrumo:
  - Asmens duomenys yra tvarkomi tik esant aiškiam ir teisėtam pagrindui, pavyzdžiui, esant darbuotojo sutikimui, vykdant sutartines prievoles, laikantis teisinių reikalavimų arba esant teisėtam įstaigos interesui.
  - Duomenų subjektas yra išsamiai informuojamas apie tai, kokie jo duomenys tvarkomi, kokiais tikslais, koks yra tvarkymo teisinis pagrindas ir kokios yra jo teisės. Visa informacija pateikiama paprasta, aiškia ir lengvai suprantama kalba.
- Tikslo apribojimo:
  - Duomenys renkami tik konkrečiais, aiškiai apibrėžtais ir teisėtais tikslais, kurie yra nurodyti šiose taisyklėse ir su kuriais duomenų subjektas yra supažindinamas.
  - Surinkti duomenys nėra vėliau tvarkomi jokiu kitu būdu, kuris neatitiktų pirminio duomenų rinkimo tikslo.
- Duomenų kiekio mažinimo:
  - Tvarkomi tik tie duomenys, kurie yra būtini ir pakankami nustatytiems duomenų tvarkymo tikslams pasiekti.
  - Vengiama rinkti perteklinę informaciją, kuri nėra reikalinga nurodytiems tikslams įgyvendinti, taip sumažinant duomenų tvarkymo apimtį ir riziką.
- Tikslumo:
  - Įstaiga užtikrina, kad asmens duomenys būtų tikslūs, išsamūs ir, jei reikia, nuolat atnaujinami.
  - Pasenę arba netikslūs duomenys yra nedelsiant ištaisomi arba sunaikinami, siekiant užtikrinti duomenų teisingumą.
- Saugojimo trukmės apribojimo:
  - Duomenys saugomi ne ilgiau, nei tai yra būtina tikslams, dėl kurių jie buvo surinkti.
  - Pasibaigus duomenų saugojimo terminui, jie yra saugiai ir neatkuriamai sunaikinami.
- Vientisumo ir konfidencialumo:
  - Siekiant apsaugoti duomenis nuo neteisėto ar atsitiktinio sunaikinimo, praradimo, pakeitimo, atskleidimo ar prieigos, įgyvendinamos tinkamos techninės, fizinės ir organizacinės saugumo priemonės.
  - Tik įgalioti darbuotojai gali turėti prieigą prie asmens duomenų, o prieigos teisės yra griežtai apribojamos pagal pareigines funkcijas.
- Atskaitomybės:
  - Įstaiga atsako už visų BDAR ir kitų susijusių teisės aktų reikalavimų laikymąsi.
  - Įstaiga privalo turėti galimybę įrodyti, kad asmens duomenys tvarkomi laikantis minėtų principų. Tam yra vedami duomenų tvarkymo veiklos įrašai, atliekamas rizikos vertinimas ir kiti atskaitomybę užtikrinantys veiksmai.

IV. SKYRIUS
TVARKYMO TIKSLAI IR TEISINIAI PAGRINDAI

9. Duomenys Įstaigoje tvarkomi šiais pagrindais ir tikslais:

Tvarkymo tikslas	Teisinis pagrindas	Pavyzdžiai
Vidaus administravimas	LR darbo kodeksas, švietimo įstatymas, sutartys	Darbuotojų duomenys, atlyginimai, atostogos
Atranka į darbo vietas	Duomenų subjekto sutikimas, sutartiniai santykiai	Gyvenimo aprašymai, kontaktiniai duomenys
Ugdymo veiklos užtikrinimas	Švietimo įstatymas, BDAR 6 str. 1 d. c punktas	Ugdytinių ir tėvų duomenys
Bendruomenės informavimas	Duomenų subjekto sutikimas	Nuotraukos, vaizdo įrašai, pasiekimai
Turto, sveikatos ir saugumo apsauga	Darbo saugos ir sveikatos įstatymas	Įėjimo registrai, incidentų žurnalai
Skundų ir prašymų nagrinėjimas	Viešojo administravimo įstatymas	Prašymų registrai, raštvedyba

V. SKYRIUS
DUOMENŲ VALDYTOJO IR TVARKYTOJO ATSAKOMYBĖ

10. Duomenų valdytojas:
- priima sprendimus dėl duomenų tvarkymo;
- užtikrina atitiktį BDAR ir ADTAĮ;
- paskiria duomenų apsaugos pareigūną;
- tvarko duomenų tvarkymo veiklos įrašus;
- praneša apie duomenų saugumo pažeidimus.

11. Duomenų tvarkytojas:
- duomenis tvarko tik pagal sutartį ir valdytojo nurodymus;
- įgyvendina saugumo priemones;
- užtikrina konfidencialumą
- praneša valdytojui apie incidentus;
- padeda vykdyti duomenų subjekto teises

VI. SKYRIUS
DUOMENŲ SUBJEKTO TEISĖS IR JŲ ĮGYVENDINIMO TVARKA

12. Duomenų subjektas turi teises:

- **Teisė žinoti ir būti informuotam:** gauti aiškią informaciją apie savo asmens duomenų tvarkymą.
- **Teisė susipažinti su duomenimis:** gauti patvirtinimą, ar su juo susiję duomenys yra tvarkomi, ir, jei taip, gauti prieigą prie šių duomenų.
- **Teisė reikalauti ištaisyti duomenis:** prašyti ištaisyti netikslius ar papildyti neišsamius duomenis.

- **Teisė reikalauti ištrinti duomenis („teisė būti pamirštam“):** reikalauti, kad duomenys būtų sunaikinti, jei jie nebereikalingi tikslams, dėl kurių buvo surinkti, arba jei atšaukiamas sutikimas.
- **Teisė apriboti duomenų tvarkymą:** reikalauti apriboti duomenų tvarkymą, jei yra ginčijamas duomenų tikslumas arba duomenys tvarkomi neteisėtai.
- **Teisė į duomenų perkeliamumą:** gauti savo duomenis susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu bei persiųsti juos kitam valdytojui, jei duomenys tvarkomi sutikimo arba sutarties pagrindu.
- **Teisė nesutikti su duomenų tvarkymu:** pareikšti nesutikimą su duomenų tvarkymu, atliekamu viešojo intereso pagrindu arba siekiant Duomenų valdytojo ar trečiosios šalies teisėtų interesų.

13. Duomenų subjektas, siekdamas pasinaudoti savo teisėmis (prieiga prie duomenų, ištaisymas, ištrynimas, apribojimas, duomenų perkeliamumas, nesutikimas su tvarkymu), į Duomenų valdytoją gali kreiptis raštu.

14. Prašymas turi būti pateiktas valstybine kalba ir būti įskaitomas.

15. Duomenų subjektas gali nurodyti pageidaujamą atsakymo gavimo būdą (el. paštu, paštu ar asmeniškai atsiimant).

16. Asmens tapatybės patvirtinimas:

- Kartu su prašymu duomenų subjektas privalo pateikti dokumentą ar kitą priemonę, patvirtinančią jo tapatybę (pvz., asmens tapatybės kortelę, pasą, elektroninį parašą).
- Jei tapatybė nėra patvirtinama, prašymas negali būti nagrinėjamas.
- Ši taisyklė netaikoma, kai asmuo kreipiasi tik dėl bendros informacijos apie duomenų tvarkymą pagal BDAR 13 ir 14 straipsnius.

17. Prašymas turi būti aiškus, tikslus ir įskaitomas, kad būtų galima tinkamai identifikuoti duomenų subjektą ir suprasti jo reikalavimus.

18. Prašymų teikimas per atstovą:

- Duomenų subjektas gali naudotis savo teisėmis ir per tinkamai įgaliotą atstovą.
- Atstovas prašyme nurodo: savo vardą, pavardę, adresą, kontaktinius duomenis bei atstovaujamo asmens duomenis (vardą, pavardę, gimimo datą).
- Privaloma pridėti dokumentą, patvirtinantį atstovavimą (įgaliojimą, globą ar kitą teisėtą pagrindą), arba jo patvirtintą kopiją.

19. Papildomos informacijos reikalavimas:

- Jei Duomenų valdytojui kyla abejonių dėl prašymą pateikusio asmens tapatybės ar pateiktų dokumentų autentiškumo, jis turi teisę paprašyti papildomos informacijos, reikalingos tapatybei nustatyti.
- Papildomos informacijos nepateikus, prašymas gali būti atmestas kaip nepagrįstas.

20. Prašymų nagrinėjimo terminai:

- Duomenų valdytojas privalo atsakyti į duomenų subjekto prašymą ne vėliau kaip per 1 mėnesį nuo jo gavimo dienos.
- Jei prašymas yra sudėtingas arba pateikta daug prašymų, šis terminas gali būti pratęstas dar 2 mėnesiams, apie tai raštu informuojant duomenų subjektą.
- Atsakymai pateikiami nemokamai, išskyrus atvejus, kai prašymai yra akivaizdžiai nepagrįsti ar pertekliniai – tuomet gali būti taikomas pagrįstas administracinis mokestis.

21. Bendravimas su duomenų apsaugos pareigūnu:

- Visais klausimais, susijusiais su asmens duomenų tvarkymu ar teisių įgyvendinimu, duomenų subjektas gali tiesiogiai kreiptis į Duomenų apsaugos pareigūną.

- Siekiant užtikrinti konfidencialumą, kreipiantis paštu ant voko būtina aiškiai pažymėti: „Skirta duomenų apsaugos pareigūnui“.

VII. SKYRIUS
DUOMENŲ APSAUGOS PAREIGŪNO ATSAKOMYBĖS IR UŽDUOTYS

22. Duomenų apsaugos pareigūnas yra atsakingas už tai, kad įstaigoje būtų tinkamai įgyvendinamos Reglamento ir kitų teisės aktų nuostatos.

23. Jo pagrindinės funkcijos apima:

- Konsultuoja Duomenų valdytoją ir darbuotojus asmens duomenų tvarkymo klausimais.
- Informuoja apie pareigas, kylančias pagal BDAR.
- Stebi, kaip įstaigoje laikomasi asmens duomenų apsaugos principų ir taisyklių.
- Rengia ir prižiūri duomenų tvarkymo veiklos įrašus.
- Yra kontaktinis asmuo Valstybinei duomenų apsaugos inspekcijai.
- Bendrauja su duomenų subjektais dėl jų teisių įgyvendinimo.

VIII. SKYRIUS
POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

24. Poveikio duomenų apsaugai vertinimas (PDAV) yra procesas, kurio metu nustatomos, analizuojamos ir vertinamos galimos asmens duomenų tvarkymo rizikos, o taip pat nustatomos priemonės šioms rizikoms sumažinti.

25. PDAV yra privalomas, kai numatomas duomenų tvarkymas gali kelti didelį pavojų duomenų subjektų teisėms ir laisvėms.

26. Vertinimas atliekamas prieš pradedant planuojamą duomenų tvarkymo veiklą.

27. PDAV atliekamas, kai numatoma vykdyti duomenų tvarkymą, kuris gali turėti reikšmingą poveikį duomenų subjektams, įskaitant, bet neapsiribojant:

- didelio masto vaizdo stebėjimo sistemas (pvz., patalpų ar teritorijų kontrolė);
- kai tvarkomi ypatingų kategorijų asmens duomenys (pvz., sveikatos duomenys);
- profiliavimą arba automatizuotus sprendimus, darančius reikšmingą įtaką duomenų subjektui (pvz., elgesio analizė, klasifikavimas);
- kai naujos technologijos gali kelti didelį pavojų duomenų subjektų teisėms;
- kai duomenys perduodami už ES ribų;
- situacijas, kurias priežiūros institucija yra įvardijusi kaip reikalaujančias PDAV atlikimo.

28. Atliekant PDAV, Duomenų valdytojas turi:

- išsamiai aprašyti planuojamas duomenų tvarkymo operacijas ir jų tikslus;
- įvertinti būtinybę ir proporcingumą tvarkymo atžvilgiu;
- nustatyti galimas rizikas duomenų subjektų teisėms ir laisvėms (pvz., neteisėtas atskleidimas, diskriminacija, duomenų praradimas);
- įvertinti šių rizikų tikimybę ir poveikio mastą;
- numatyti konkrečias technines ir organizacines priemones rizikoms sumažinti (pvz., šifravimas, pseudonimizacija, prieigos ribojimas);

- įvertinti, ar numatytos priemonės yra pakankamos užtikrinti BDAR reikalavimų laikymąsi.

29. Už PDAV atlikimą atsako Duomenų valdytojas, tačiau procese dalyvauja Duomenų apsaugos pareigūnas, teikiantis konsultacijas.

30. Jei tvarkymą vykdo keli valdytojai, PDAV atliekamas bendradarbiaujant.

31. PDAV rezultatai turi būti dokumentuojami raštu (popieriuje arba elektroniniu formatu).

32. Dokumentacija saugoma Įstaigos duomenų apsaugos byloje ir turi būti pateikiama priežiūros institucijai paprašius.

33. Jei atlikus PDAV nustatoma, kad numatyto duomenų tvarkymo rizika išlieka didelė, nepaisant planuojamų apsaugos priemonių, Duomenų valdytojas privalo kreiptis į Valstybinę duomenų apsaugos inspekciją dėl konsultacijos (BDAR 36 str.).

34. PDAV turi būti atnaujinamas:

- pasikeitus tvarkymo tikslams ar priemonėms;
- pasikeitus naudojamoms technologijoms;
- pasikeitus teisės aktų reikalavimams;
- nustačius naujas grėsmes ar įvykus incidentui.

35. Jei tvarkymas yra nuolatinio pobūdžio, PDAV rekomenduojama peržiūrėti ne rečiau kaip kas 3 metus.

IX. SKYRIUS
DUOMENŲ TVARKYTOJO PASITELKIMAS IR JO PAREIGOS

36. Pasitelkus duomenų tvarkytoją, Duomenų valdytojas ir Duomenų tvarkytojas privalo sudaryti rašytinę sutartį, kurioje numatomos abiem šalims privalomos nuostatos.

37. Rašytinė (popierinė arba elektroninė) sutartis, apima:

- tvarkymo objektas, trukmė, pobūdis ir tikslai;
- tvarkomų asmens duomenų rūšys ir duomenų subjektų kategorijos;
- tvarkytojo įsipareigojimas tvarkyti duomenis tik pagal dokumentuotus Duomenų valdytojo nurodymus;
- įsipareigojimas užtikrinti, kad duomenis tvarkytų tik įgalioti asmenys, pasirašę konfidencialumo pasižadėjimus;
- techninių ir organizacinių saugumo priemonių aprašymas;
- sub-tvarkytojų pasitelkimo sąlygos (tik su išankstiniu Duomenų valdytojo sutikimu);
- įsipareigojimas padėti Duomenų valdytojui įgyvendinti jo prievoles (duomenų subjektų teisių užtikrinimą, poveikio vertinimą, incidentų valdymą);
- duomenų ištrynimo ar grąžinimo procedūra pasibaigus sutarties galiojimui;
- galimybė Duomenų valdytojui atlikti auditą ar patikrą, vertinant sutarties vykdymą.

38. Duomenų tvarkytojas turi šias pagrindines pareigas:

- įgyvendinti tinkamas technines, organizacines ir fizines saugumo priemones, užtikrinančias duomenų konfidencialumą, vientisumą ir prieinamumą;
- duomenis tvarkyti tik pagal Duomenų valdytojo nurodymus ir nekeisti jų tvarkymo tikslo ar apimties savo nuožiūra;

- užtikrinti, kad duomenis tvarkytų tik tie darbuotojai, kuriems suteikta prieiga pagal „mažiausios būtinos prieigos“ principą;
- padėti Duomenų valdytojui įgyvendinti duomenų subjektų teises (prieigos, ištaisymo, ištrynimo, apribojimo, perkeliamumo);
- padėti Duomenų valdytojui laikytis duomenų saugumo pažeidimų pranešimo prievolių;
- tvarkyti incidentų žurnalus ir nedelsiant pranešti Duomenų valdytojui apie bet kokius duomenų saugumo pažeidimus;
- laikytis konfidencialumo principo ir neatskleisti tvarkomų duomenų jokiems tretiesiems asmenims be Duomenų valdytojo leidimo;
- pasibaigus sutarčiai, visus tvarkytus duomenis grąžinti Duomenų valdytojui arba saugiai ištrinti, išskyrus atvejus, kai įstatymai įpareigoja juos saugoti.

39. Sub-tvarkytojų pasitelkimas:
- Duomenų tvarkytojas gali pasitelkti kitą tvarkytoją (sub-tvarkytoją) tik gavęs išankstinį rašytinį Duomenų valdytojo sutikimą.
- Sub-tvarkytojas privalo laikytis tokių pačių pareigų ir reikalavimų, kokie nustatyti pagrindiniam tvarkytojui.
- Už sub-tvarkytojo veiksmus prieš Duomenų valdytoją atsako **pagrindinis duomenų tvarkytojas**.

40. Atsakomybė:
- Duomenų tvarkytojas atsako už tai, kad jo veikla neprieštarautų BDAR, ADTAĮ ir šių taisyklių nuostatoms.
- Jei tvarkytojas viršija jam suteiktus įgaliojimus ir pradeda veikti savo nuožiūra, jis laikomas duomenų valdytoju ir už padarytą žalą atsako kaip valdytojas.

X. SKYRIUS
DUOMENŲ PERDAVIMAS TRETIESIEMS ASMENIMS IR UŽ ES RIBŲ

41. Duomenų perdavimas tretiesiems asmenims (juridiniams ar fiziniams, kurie nėra Duomenų valdytojo darbuotojai) galimas tik tuo atveju, kai:
- yra aiškus ir teisėtas teisinis pagrindas (įstatymas, sutartis, teisėtas interesas);
- tai būtina Įstaigos funkcijų vykdymui (pvz., finansinės apskaitos tvarkymui, viešųjų paslaugų teikimui);
- duomenų subjektas davė aiškų sutikimą, jeigu duomenų teikimas grindžiamas jo valia.

42. Perduodant už ES ribų užtikrinamos BDAR numatytos garantijos (standartinės sutarčių sąlygos, priežiūros institucijos leidimas).

43. Trečiosioms šalims perduodami tik tie duomenys, kurie yra būtini numatytam tikslui pasiekti, laikantis duomenų kiekio mažinimo principo.

44.Įstaiga gali perduoti asmens duomenis šiems subjektams:
- valstybės institucijoms ir priežiūros įstaigoms, turinčioms teisę gauti duomenis pagal įstatymus (pvz., VMI, „Sodra“, teisėsaugos institucijos);
- partneriams ar paslaugų teikėjams, kurie teikia Įstaigai būtinas paslaugas (pvz., IT infrastruktūros priežiūra, archyvavimo paslaugos, buhalterinė apskaita);

- kitoms švietimo, mokslo ar socialinės apsaugos įstaigoms, kai tai būtina vaiko ugdymo ar socialinės paramos procesams.

45. Kiekvienu atveju duomenų gavėjas įsipareigoja:

- tvarkyti gautus duomenis tik nurodytu tikslu;
- įgyvendinti BDAR atitinkančias technines ir organizacines priemones;
- užtikrinti duomenų konfidencialumą.

46. Draudimai ir apribojimai:

- Draudžiama perduoti duomenis valstybėms, kurios neužtikrina tinkamos apsaugos, jei nėra taikomos papildomos BDAR priemonės.
- Draudžiama perduoti daugiau duomenų nei yra būtina numatytam tikslui.
- Draudžiama naudoti trečiuosius tvarkytojus ar gavėjus, kurie negali užtikrinti tinkamo saugumo lygio.

47. Duomenų subjekto informavimas jei duomenys perduodami už ES ribų :

- valstybę ar tarptautinę organizaciją, kuriai duomenys bus perduodami;
- taikomas apsaugos priemones (pvz., standartines sutarties sąlygas, Komisijos sprendimą dėl tinkamumo);
- galimas rizikas.

XI. SKYRIUS
SAUGUMO PRIEMONĖS

48. Įstaiga įgyvendina išsamias technines, organizacines ir fizines priemones, kad užtikrintų asmens duomenų vientisumą, konfidencialumą ir prieinamumą.

49. Techninės priemonės:

- Naudojama stipri slaptažodžių politika: slaptažodžiai privalo būti ne trumpesni nei 8 simboliai, keičiasi ne rečiau kaip kas 90 dienų, negali sutapti su asmeniniais duomenimis (pvz., vardu, gimimo data).
- Įrenginiuose įdiegtos ugniasienės ir antivirusinės sistemos, kurios reguliariai atnaujinamos.
- Duomenys, saugomi elektroninėse laikmenose, apsaugoti šifravimo priemonėmis, ypač jautri informacija šifruojama tiek perduodant, tiek saugant.
- Atliekamos reguliarios atsarginės kopijos, kurios laikomos atskirose saugiose laikmenose.
- Įstaigoje užtikrinamas apsaugotas interneto ryšys; bevieliai tinklai naudojami tik su stipriu šifravimu (WPA2 ar naujesniu).
- Nenaudojamos laikmenos ar diskai prieš išmetimą yra fiziškai sunaikinami arba jų duomenys ištrinami naudojant sertifikuotus ištrynimo metodus.

50. Organizacinės priemonės:

- Visi darbuotojai, tvarkantys duomenis, yra supažindinti su konfidencialumo įsipareigojimais ir pasirašo atitinkamus dokumentus.
- Darbuotojams suteikiama tik tokia prieiga, kuri yra būtina jų funkcijoms vykdyti (principas „mažiausia būtina prieiga“).
- Įdiegta prieigos teisių suteikimo ir atėmimo procedūra: pasikeitus darbuotojo pareigoms ar jam išėjus iš darbo, prieiga prie duomenų nedelsiant nutraukiama.

- Vykdomi periodiniai mokymai darbuotojams apie BDAR reikalavimus, saugų elgesį su duomenimis, kibernetinių grėsmių prevenciją.
- Įgyvendinami incidentų valdymo planai: darbuotojai žino, kaip veikti pastebėjus galimą duomenų saugumo pažeidimą.
- Įstaigoje nustatyta tvarka, kaip reguliariai peržiūrėti ir atnaujinti duomenų tvarkymo politiką, atsižvelgiant į naujas technologijas ar kylančias rizikas.
- Atlikus vidinius auditų patikrinimus, dokumentuojamos pastabos ir koreguojamos saugumo procedūros.

51. Fizinės priemonės:

- Patalpos, kuriose saugomi asmens duomenys, yra užrakinamos ir prieinamos tik įgaliotiems darbuotojams.
- Dokumentai su asmens duomenimis laikomi užrakintose spintose, seifuose ar archyvavimo patalpose, kur prieiga ribojama.
- Esant poreikiui, naudojamos vaizdo stebėjimo priemonės, laikantis proporcingumo principo ir BDAR reikalavimų.
- Popieriniai dokumentai, kurių saugojimo terminas pasibaigė, yra sunaikinami specialiais smulkintuvais arba perduodami sertifikuotai dokumentų naikinimo paslaugai.
- Darbuotojai privalo užtikrinti, kad darbo vietoje nebūtų palikti atviri dokumentai ar įjungti kompiuteriai su atidarytais duomenimis be priežiūros.

52. Papildomos priemonės:

- Duomenų apsaugos pareigūnas vertina rizikas ir teikia rekomendacijas dėl papildomų priemonių taikymo.

XII. SKYRIUS
DUOMENŲ SAUGUMO INCIDENTAI

53. Asmens duomenų saugumo incidentu laikomas bet koks įvykis, dėl kurio:

- duomenys yra prarandami, sunaikinami arba sugadinami;
- duomenys tampa neleistinai atskleisti ar pasiekiami asmenims, neturintiems teisės juos gauti;
- duomenys yra pakeisti be teisėto pagrindo;
- pažeidžiamas jų konfidencialumas, prieinamumas ar vientisumas.

54. Atsakomybė už incidentų nustatymą:

- Incidentą pastebėjęs darbuotojas nedelsdamas privalo informuoti Duomenų apsaugos pareigūną arba Įstaigos vadovą.
- Duomenų apsaugos pareigūnas atsako už incidento registravimą, tyrimą, rizikos įvertinimą ir sprendimo dėl pranešimo priėmimą.
- Incidentų valdymo procesas dokumentuojamas ir saugomas Įstaigos vidaus sistemose.

55. Pranešimo priežiūros institucijai tvarka:

- Apie kiekvieną asmens duomenų pažeidimą, kuris gali sukelti pavojų duomenų subjektų teisėms ar laisvėms, Įstaiga privalo pranešti Valstybinei duomenų apsaugos inspekcijai per 72 valandas nuo sužinojimo apie incidentą.

- Pranešime turi būti nurodyta: incidento pobūdis ir mastas, paveiktų duomenų subjektų skaičius ir duomenų kategorijos, tikėtinos pasekmės, taikytos ar planuojamos taikyti priemonės, skirtos pasekmėms pašalinti ar sumažinti, kontaktiniai asmens duomenys, su kuriuo priežiūros institucija gali susisiekti.
- Jei per 72 val. neįmanoma pateikti visos informacijos, Įstaiga pateikia pradinę informaciją ir papildomą informaciją pateikia nedelsdama.

56. Jeigu incidentas gali sukelti **didelę riziką** duomenų subjektų teisėms ar laisvėms, Įstaiga privalo:
- tiesiogiai informuoti paveiktus asmenis aiškia ir paprasta kalba;
- nurodyti incidento pobūdį, galimas pasekmes ir taikytas apsaugos priemones;
- pateikti kontaktus, kuriais galima kreiptis dėl papildomos informacijos.

57. Informavimas duomenų subjektams nebūtinas, jeigu:
- duomenys buvo tinkamai šifruoti ar kitaip apsaugoti, todėl yra neįskaitomi;
- buvo nedelsiant įgyvendintos priemonės, pašalinusios riziką duomenų subjektų teisėms;
- informavimas reikalautų neproporcingų pastangų (tokiu atveju informacija gali būti pateikta viešai).

58. Po kiekvieno incidento Įstaiga privalo atlikti analizę ir imtis priemonių, kad ateityje tokie įvykiai nepasikartotų:
- peržiūrėti ir atnaujinti saugumo priemones;
- organizuoti papildomus darbuotojų mokymus;
- patikrinti trečiųjų paslaugų teikėjų saugumo procedūras;
- sustiprinti techninę apsaugą (pvz., diegti dviejų faktorių autentifikaciją, griežtinti prieigos kontrolę).

XIII. SKYRIUS
DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI IR PRIEŽIŪRA

59. Įstaiga privalo tvarkyti visų asmens duomenų tvarkymo veiklų įrašus, kaip tai numato BDAR 30 straipsnis.

60. Įrašai sudaromi ir prižiūrimi rašytine forma, kuri gali būti tiek popierinė, tiek elektroninė.

61. Įrašai laikomi įstaigos dokumentų valdymo sistemoje ir yra prieinami Duomenų apsaugos pareigūnui bei priežiūros institucijai pagal pareikalavimą.

62. Kiekvienas įrašas privalo apimti bent šiuos duomenis:
- duomenų valdytojo pavadinimas, juridinis kodas ir kontaktiniai duomenys;
- duomenų apsaugos pareigūno kontaktiniai duomenys;
- tvarkymo tikslai;
- duomenų subjektų kategorijos;
- tvarkomų asmens duomenų kategorijos;
- duomenų gavėjai ar jų grupės, įskaitant gavėjus už ES/EEE ribų;
- duomenų saugojimo terminai;
- techninės, organizacinės ir fizinės priemonės, skirtos apsaugoti duomenis.

63. Už įrašų tvarkymą atsakingas Įstaigos vadovo paskirtas asmuo.

64. Darbuotojai, vykdantys duomenų tvarkymo operacijas, privalo laiku teikti visą informaciją, reikalingą įrašams pildyti ir atnaujinti.

65. Už pateiktų duomenų tikslumą atsako kiekvienas duomenų tvarkymą atliekantis darbuotojas.

66. Įrašai peržiūrimi ne rečiau kaip kartą per dvejus metus, taip pat kiekvieną kartą pasikeitus:

- teisės aktų reikalavimams;
- duomenų tvarkymo procesams ar tikslams;
- naudojamoms technologijoms;
- duomenų gavėjams ar tvarkytojams.

67. Peržiūros metu nustatyti neatitikimai turi būti pašalinti nedelsiant.

68. Valstybinei duomenų apsaugos inspekcijai paprašius, Įstaiga privalo nedelsiant pateikti atnaujintus įrašus.

69. Pateikiami įrašai turi būti suprantami, išsamūs ir aiškiai parengti, kad institucija galėtų įvertinti tvarkymo teisėtumą.

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

70. Duomenų valdytojo ar duomenų tvarkytojo darbuotojai, turintys prieigos prie asmens duomenų teisę, pastebėję duomenų saugumo pažeidimus ar bet kokią įtartiną situaciją (veiksmus ar neveikimą, galinčius sukelti ar sukeliančius grėsmę asmens duomenų saugumui), turi imtis priemonių tokiai situacijai išvengti ir apie tai informuoti Duomenų valdytojo vadovą, duomenų apsaugos pareigūną ar kitą paskirtą atsakingą asmenį.

71. Įvertinus duomenų apsaugos pažeidimo rizikos veiksnius, pažeidimo poveikio laipsnį, žalą ir padarinius, kiekvienu konkrečiu atveju Įstaigos vadovas priima sprendimus dėl priemonių, reikiamų duomenų apsaugos pažeidimui ir jo padariniams pašalinti.

72. Prireikus, Įstaigos vadovas, duomenų apsaugos pareigūnas ar kitas paskirtas atsakingas asmuo imasi pareigos užtikrinti, kad apie duomenų/ informacijos saugumo pažeidimus būtų pranešta (ne vėliau kaip per 72 val. nuo sužinojimo apie pažeidimą) Asmens duomenų apsaugos inspekcijai ir/ar teisėsaugos institucijoms ir susijusiems asmenims, laikantis Reglamento, ADTAĮ ir kitų teisės aktų reikalavimų.

XV. SKYRIUS
BAIGIAMOSIOS NUOSTATOS0

73. **Taisyklių privalomumas:** Šios asmens duomenų tvarkymo taisyklės yra privalomos visiems Įstaigos darbuotojams, praktikantams ir kitiems asmenims, kurie, vykdydami savo pareigas, turi prieigą prie įstaigos tvarkomų asmens duomenų.

74. **Atsakomybė už pažeidimus:** Už šių Taisyklių, Lietuvos Respublikos įstatymų ar ES Reglamento pažeidimus asmenys atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

75. **Supažindinimas su Taisyklėmis:** Su šiomis Taisyklėmis ir jų pakeitimais nauji darbuotojai privalo būti supažindinti pasirašytinai, ne vėliau kaip pirmąją darbo dieną. Esami darbuotojai su atnaujintomis Taisyklėmis supažindinami nedelsiant, kai tik jos įsigalioja.

76. **Taisyklių peržiūra ir atnaujinimas:** Taisyklės yra nuolat peržiūrimos ir atnaujinamos, atsižvelgiant į besikeičiančius teisės aktus, teismų praktiką, Valstybinės duomenų apsaugos inspekcijos rekomendacijas bei įstaigos veiklos ypatumus. Rekomenduojama Taisykles peržiūrėti ne rečiau kaip kas dvejus metus, siekiant užtikrinti jų aktualumą ir atitiktį galiojančiai teisinei bazei.

77. Priežiūra ir kontrolė: Už Taisyklių vykdymo priežiūrą ir kontrolę atsakingas įstaigos direktorius arba jo įsakymu paskirtas asmuo (pvz., duomenų apsaugos pareigūnas).

78. **Ginčų sprendimas:** Kilus ginčams dėl asmens duomenų tvarkymo, jie sprendžiami derybų keliu. Nepavykus susitarti, ginčai sprendžiami Lietuvos Respublikos teisės aktų nustatyta tvarka.

79. **Įsigaliojimas:** Šios Taisyklės įsigalioja nuo jų patvirtinimo įstaigos direktoriaus įsakymu dienos.