VILNIAUS LOPŠELIO – DARŽELIO „KRIVŪLĖ“
JURIDINIO ASMENS KODAS 190015782

PATVIRTINTA
Vilniaus lopšelis – darželis „Krivūlė“
direktoriaus
2019 m. birželio 19 d. įsakymu Nr. V-207

ASMENS DUOMENŲ SAUGOJIMO POLITIKA

I. BENDROSIOS NUOSTATOS, TIKSLAS

1. Vilniaus lopšelis – darželis „Krivūlė“ (toliau – „**Įstaiga**“), vykdydama savo veiklą, nuolat renka ir tvarko tam tikrą informaciją ir duomenis apie duomenų subjektus. Informacija gali apimti įstaigos darbuotojus, siekiančius įsidarbinti asmenis, vaikus ir jų tėvus, ir kitus fizinius asmenius, su kuriais įstaigai gali tekti bendradarbiauti įvairiais klausimais.

2. Ši politika nustato, kaip asmens duomenys turi būti renkami, tvarkomi, naudojami ir saugomi, kad atitiktų Bendrąjį duomenų apsaugos reglamentą Nr. 2016/679 (ES), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymą ir kitus teisės aktus, įstaigos asmens duomenų saugojimo standartus.

3. Ši politika užtikrina, kad Įstaiga:

3.1. laikosi visų asmens duomenų apsaugos teisės aktų ir palaiko gerąją praktiką šioje srityje;

3.2. saugo ir gerbia darbuotojų, siekiančių įsidarbinti asmenų, vaikų ir jų tėvų/globėjų, ir kitų fizinių asmenų teises;

3.3. yra atvira dėl to, kaip ji saugo ir apdoroja asmens duomenis;

3.4. saugo save nuo asmens duomenų pažeidimo pavojaus.

4. Šia politika užtikrinama, kad Įstaigos darbuotojai yra supažindinti ir supranta esmines taisykles, reglamentuojančias asmens duomenų, prie kurių jie turi prieigą savo darbo metu, tvarkymą.

II. POLITIKOS TAIKYMO SRITIS

5. Ši politika yra privaloma visiems Įstaigos darbuotojams, siekiantiems įsidarbinti asmenims, vaikams ir jų tėvams ir kitiems asmenims, dirbantiems ar veikiantiems Įstaigos vardu.

6. Ši politika taikoma visiems Įstaigos turimiems duomenims, susijusiems su identifikuojamais fiziniais asmenimis. Tai gali būti asmeniniai duomenys, kontaktiniai ir kiti duomenys.

7. Be šios politikos, darbuotojai privalo vadovautis šiais teisės aktais:

7.1. Europos Parlamento ir Tarybos Reglamentu Nr. 2016/679 (ES), priimtu 2016 m. balandžio 27 d., dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB.

7.2. Europos Tarybos konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (Nr. 108).

7.3. Europos žmogaus teisių ir pagrindinių laisvių konvencija.

7.4. Lietuvos Respublikos Konstitucija;

7.5. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

7.6. kitais teisės aktais, kurie reglamentuoja asmens duomenų apsaugą.

III. PAGRINDINIAI APIBRĖŽIMAI IR SĄVOKOS

8. Šioje politikoje vartojamos šios pagrindinės sąvokos:

8.1. **Asmens duomenys arba duomenys** – bet kokia informacija apie duomenų subjektą, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti;

8.2. **Duomenų subjektas** – bet koks fizinis asmuo, kurio tapatybę galima nustatyti tiek tiesiogiai, tiek netiesiogiai iš turimų duomenų, tokių kaip, pavyzdžiui, vardo, pavardės, asmens kodo, gyvenamojo adreso, IP adreso, vieno ar kelių genetinių, fiziologinių, psichinių, ekonominių, kultūrinių ar socialinių duomenų ir pan.

8.3. **Įstaiga** – duomenų valdytojas: Vilniaus lopšelis – darželis „Krivūlė“ juridinio asmens kodas 190015782, visi jos filialai, padaliniai, skyriai ar kiti struktūriniai vienetai.

8.4. **Darbuotojas(-ai) –** fizinis asmuo, kuris sudarė darbo sutartį su Įstaiga.

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

8.6. **Asmens užklausa** – asmens prašymas, skirtas Įstaigai, pateikti informaciją apie su juo susijusius duomenis ir (arba) imtis kitų veiksmų su jo asmens duomenų tvarkymu.

8.7. **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.

8.8. **Trečioji šalis ar trečiasis asmuo** – fizinis arba juridinis asmuo, valdžios institucija, įmonė ar kita organizacija, kuri nėra duomenų subjektas, duomenų valdytojas, duomenų tvarkytojas, arba asmenys, kuriems tiesioginiu Įstaigos įgaliojimu leidžiama tvarkyti asmens duomenis.

9. Kitos šioje politikoje nepaminėtos sąvokos gali būti įtvirtintos Bendrajame duomenų

apsaugos reglamente Nr. 2016/679 (ES), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme ir kituose teisės aktuose.

IV. ATSAKOMYBĖ

10. Kiekvienas asmuo, kuris dirba Įstaigoje arba kartu su Įstaiga, veikia Įstaigos vardu, yra atsakingas už tinkamą ir teisėtą tvarkomų asmens duomenų rinkimą, naudojimą, tvarkymą, saugumą ir perdavimą.

11. Kiekvienas asmuo ar asmenų grupė, kuri tvarko asmens duomenis, turi užtikrinti, kad duomenys tvarkomi vadovaujantis šia politika ir pagrindiniais asmens duomenų apsaugos principais.

12. Pagrindinės atsakomybės sritys:

12.1. Įstaigos direktorius yra atsakingas už visų duomenų tvarkymą Įstaigoje.

12.2. Įstaigos sekretorė yra atsakinga už:

12.2.1. viso personalo supažindinimą apie Įstaigos ir jos darbuotojų pareigas, atsakomybę, potencialią riziką asmens duomenų apsaugos srityje;

12.2.2. visų asmens duomenų tvarkymo apsaugos procedūrų peržiūrą ir kontrolę, susijusių veiksmų ir krypčių nustatymą;

12.2.3. asmenų, dirbančių Įstaigoje ar kartu su ja, veikiančių Įstaigos vardu, apmokymų organizavimą pagal poreikį ir nuolatinių rekomendacijų teikimą asmens duomenų tvarkymo ir apsaugos klausimais;

12.2.4. duomenų subjektų užklausų ir kitų prašymų nagrinėjimą ir atsakymą į užklausas;

12.2.5. bet kokių sutarčių ar susitarimų su trečiaisiais asmenims, kurie gali tvarkyti konfidencialius Įstaigoje turimus asmens duomenis, sudarymą ir šių sutarčių ar susitarimų kontrolę.

12.2.6. siunčiamus paprastus ar elektroninius laiškus, kuriuose gali būti naudojami asmens duomenys.

12.3 IT specialistas yra atsakingas už:

12.3.1. tai, kad visos IT sistemos, kompiuterinės programos, įranga, kurie naudojami asmens duomenims tvarkyti, saugoti, atitiktų priimtinus saugumo standartus (įskaitant naudojamų techninių išteklių saugumą, techninę priežiūrą ir pan.);

12.3.2. reguliarius ir nuolatinius programų patikrinimus ir nuskaitymus (skenavimus), užtikrinant tinkamą naudojamos programinės įrangos veikimą ir saugumą;

12.3.3.visų naudojamų IT resursų apsaugą nuo bet kokių grėsmių;

12.3.4. išorinių IT paslaugų teikėjų vertinimą, kuriems gali būti perduodami Įstaigoje turimi asmens duomenys.

V. ASMENS DUOMENŲ SAUGOJIMO PRINCIPAI

13. Įstaiga turi tvarkyti asmens duomenis sąžiningai ir teisėtai, laikydamasi duomenų subjektų teisių. Įstaiga neturėtų tvarkyti perteklinių asmens duomenų, išskyrus atvejus, kai asmuo, kurio duomenys yra tvarkomi, sutinka dėl tokių duomenų tvarkymo. Įstaiga privalo tvarkyti asmens duomenis laikydamasi pagrindinių asmens duomenų tvarkymo ir saugojimo principų.

14. Pagrindiniai asmens duomenų tvarkymo principai:

14.1. asmens duomenys turi būti tvarkomi tiksliai, sąžiningai ir teisėtai;

14.2. asmens duomenys turi būti gaunami tik konkrečiais, teisėtais tikslais;

14.3. asmens duomenys turi būti tinkami, reikalingi ir ne pertekliniai;

14.4. asmens duomenys turi būti tikslūs ir, jei reikia asmens duomenų tvarkymui, nuolat atnaujinami;

14.5. asmens duomenys turi būti saugomi ne ilgiau, nei to reikalauja duomenų tvarkymo tikslai;

14.6. asmens duomenys turi būti tvarkomi nepažeidžiant duomenų subjektų teises;

14.7. asmens duomenys turi būti saugomi tinkamais būdais ir priemonėmis;

14.8. asmens duomenys negali būti perduodami už Europos Sąjungos ribų, nebent tos valstybės, kuriai perduodami duomenys, subjektas taip pat gali užtikrinti tinkamą asmens duomenų tvarkymo ir apsaugos lygį.

15. Įstaiga turėtų fiksuoti (registruoti, dokumentuoti) kiekvieną papildomą naujų asmens duomenų apdorojimo pagrindimą ir užtikrinti, kad visi biometriniai ir genetiniai duomenys būtų laikomi jautriais (specialiosios kategorijos duomenimis).

16. Jeigu Įstaiga renka tam tikrus duomenis neturint tam teisinio pagrindo, Įstaiga tokiu atveju turi gauti duomenų subjekto sutikimą. Šis sutikimas gali būti atšauktas arba panaikintas bet kuriuo metu.

VI. ASMENS DUOMENŲ SAUGOJIMO RIZIKA

17. Ši politika padeda apsaugoti įstaigą nuo duomenų saugumo rizikos, įskaitant:

17.1. bendrojo duomenų apsaugos reglamento Nr. 2016/679 (ES) pažeidimus;

17.2. konfidencialumo pažeidimus (pavyzdžiui, neteisingai pateikiama informacija ir kt.);

17.3. žalą, padarytą Įstaigos dalykinei reputacijai (pavyzdžiui, Įstaiga gali nukentėti nuo kibernetinio įsilaužimo,įsilaužėliams sėkmingai gaunant prieigą prie asmens duomenų ir kt.).

VII. BENDROSIOS DUOMENŲ TVARKYMO GAIRĖS

18. Vieninteliai asmenys, kurie gali turėti prieigą prie asmens duomenų, turi būti Įstaigos darbuotojai ar kiti su Įstaiga dirbantys ar Įstaigos vardu veikiantys asmenys, kuriems asmens duomenys reikalingi dėl jų atliekamų pareigų, funkcijų ar vykdomos veiklos.

19. Duomenys negali būti perduodami neformaliai. Jeigu darbuotojams yra reikalinga prieiga prie konfidencialios informacijos ar tam tikrų duomenų, darbuotojai, nurodydami priežastį ir

pagrindą, turi prašyti tokią informaciją ar duomenis gauti iš tiesioginio vadovo.

20. Įstaiga nuolat konsultuoja ir, esant poreikiui, apmoko visus darbuotojus ir kitus asmenis dėl asmens duomenų tvarkymo, kad padėtų jiems suprasti jų atsakomybę tvarkant duomenis.

21. Darbuotojai turėtų saugoti visus turimus asmens duomenis, imdamiesi protingų ir racionalių saugumo priemonių bei laikydamiesi šios politikos ir kitų Įstaigos taisyklių.

22. Darbuotojai privalo naudoti tvirtus slaptažodžius, kuriais niekada neturėtų būti dalijamasi.

23. Duomenys neturi būti atskleisti tretiesiems asmenims tiek Įstaigos viduje, tiek išorėje, už Įstaigos ribų.

24. Duomenys turėtų būti reguliariai peržiūrimi ir tikslinami, atnaujinami, jei nustatoma, kad jie yra pasenę, netikslūs ar neaktualūs. Jei nustatoma, kad asmens duomenys yra nereikalingi, jie turėtų būti ištrinti ir sunaikinti.

25. Darbuotojai turi kreiptis pagalbos ar papildomos informacijos pas tiesioginį vadovą, jeigu jie nežino kaip elgtis tam tikrose situacijose tvarkant asmens duomenis.

VIII. ASMENS DUOMENŲ SAUGOJIMAS

26. Asmens duomenys turi būti saugomi itin saugiai.

27. Duomenys gali būti saugomi:

27.1. popieriuje (dokumentuose, sutartyse ir kt.);

27.2. elektroniniu būdu (skaitmeninėje laikmenoje).

28. Tais atvejais, kai asmens duomenys užfiksuoti popierinėje laikmenoje (dokumentuose, sutartyse ir kt.), šie dokumentai turėtų būti laikomi saugioje vietoje, apribojant priėjimą prie jų kitiems asmenims.

29. Dokumentus ar kitas popierines laikmenas, kuriuose yra užfiksuoti tam tikri asmens duomenys, kai jie nėra reikalingi, būtina susmulkinti ir sunaikinti, jog nebūtų įmanoma atstatyti jose esančią informaciją.

30. Elektroniniai asmens duomenys turėtų būti laikomi tokiuose įrenginiuose, kurie būtų apsaugoti tvirtais ir unikaliais slaptažodžiais. Slaptažodžiai turi būti reguliariai keičiami, jais griežtai negalima dalintis su kitais asmenimis.

31. Duomenys, saugomi tokiose skaitmeninėse laikmenose, kaip kompaktiniai diskai, atminties kortelės ir pan., turi būti apsaugoti nuo kitų asmenų priėjimų prie jų, saugiai užrakinti, kai jie nenaudojami.

32. Serveriai, kuriuose yra asmens duomenys, turi būti saugioje vietoje.

33. Duomenys tiesiogiai ir lengvai prieinami neturėtų būti saugomi mobiliuose įrenginiuose.

34. Visi serveriai, kuriuose yra asmens duomenys, turi būti apsaugoti specialia saugumo programine įranga ir stipria užkarda.

IX. ASMENS DUOMENŲ NAUDOJIMAS

35. Darbuotojų naudojamų kompiuterių ar kitų įrenginių ekranai, kai kompiuteriai ar kiti įrenginiai lieka be priežiūros, visada turėtų būti užrakinti.

36. Asmens duomenimis neturėtų būti dalijamasi paprastai, lengvabūdiškai ir neformaliai. Asmens duomenys neturėtų būti paprastai ir atvirai siunčiami elektroniniu paštu ar per socialinius tinklus, kadangi toks duomenų siuntimas nėra saugus.

37. Prieš elektroninį duomenų perdavimą, duomenys turi būti užšifruoti.

38. Duomenys neturėtų būti perduodami už Europos Sąjungos ribų.

39. Darbuotojai savo asmeniniuose kompiuteriuose ar kituose įrenginiuose neturėtų išsaugoti asmens duomenų kopijų.

X. ASMENS DUOMENŲ TIKSLUMAS

40. Įstaigoje turi būti laikomi ir tvarkomi tikslūs, reikalingi bei aktualūs asmens duomenys, todėl visi darbuotojai ir kiti asmenys, kurie dirba su asmens duomenimis, yra atsakingi už tai, kad būtų užtikrinta, jog asmens duomenys būtų kuo tikslesni ir, kiek įmanoma, naujausi.

41. Siekiant užtikrinti asmens duomenų tikslumą:

41.1. duomenys turėtų būti laikomi kompaktiškai, užimant kuo mažiau vietos. Įstaigos darbuotojai neturėtų kurti nereikalingų papildomų duomenų rinkinių;

41.2. darbuotojai turėtų pasinaudoti visomis galimybėmis, kad duomenys nuolat būtų atnaujinami (pavyzdžiui, atnaujinti duomenis skambučio ar susirašinėjimo metu);

41.3. Įstaiga turėtų duomenų subjektams sudaryti sąlygas atnaujinti savo duomenis, kuriuos turi Įstaiga;

41.4. duomenys turėtų būti atnaujinami, jeigu yra aptikti tam tikri netikslumai.

XI. ASMENŲ UŽKLAUSOS IR PRAŠYMAI

42. Duomenų subjektas, kurio duomenys yra tvarkomi Įstaigos veikloje, turi šias teises:

42.1. žinoti (būti informuotas) apie savo duomenų tvarkymą (teisė žinoti);

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

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

42.4. savo duomenis sunaikinti arba sustabdyti savo duomenų tvarkymo veiksmus (išskyrus saugojimą) (teisė sunaikinti ir teisė „būti pamirštam“);

42.5. reikalauti, kad Įstaiga apribotų asmens duomenų tvarkymą esant vienai iš teisėtų priežasčių (teisė apriboti);

42.6. teisę į duomenų perkėlimą (teisė perkelti);

42.7. teisę nesutikti, kad būtų tvarkomi jo asmens duomenys ar bet kada atšaukti savo

sutikimą tvarkyti asmens duomenis, kad asmens duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais, nedarant poveikio sutikimu grindžiamo duomenų tvarkymo iki sutikimo atšaukimo teisėtumui.

43. Duomenų subjektų užklausos ir prašymai gali būti pateikiami raštu, persiunčiant juos adresu: Lydos g. 5, Vilnius, arba elektroniniu paštu: rastine@krivule.vilnius.lm.lt. Prieš pateikdama bet kokią informaciją duomenų subjektui, Įstaiga privalo visada patikrinti ir įsitikinti dėl duomenų subjekto tapatybės.

44. Duomenų subjektas turi teisę kreiptis į Įstaiga ir gauti su juo susijusius asmens duomenis susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu. Šie prašymai turėtų būti išnagrinėti per 1 (vieną) mėnesį. Prireikus šis laikotarpis gali būti pratęstas dar 2 (dviem) mėnesiams, atsižvelgiant į prašymų sudėtingumą ir skaičių. Įstaiga per 1 (vieną) mėnesį nuo prašymo gavimo informuoja duomenų subjektą apie tokį pratęsimą, kartu pateikdamas vėlavimo priežastis. Duomenų subjektas taip pat gali pareikalauti, kad jo duomenys būtų tiesiogiai perkelti į kitą sistemą.

45. Įstaiga pateikia informaciją arba bet kokį kitą pranešimą ar atlieka su tuo susijusius veiksmus nemokamai. Kai duomenų subjekto prašymai yra akivaizdžiai nepagrįsti arba neproporcingi, visų pirma dėl jų pasikartojančio turinio, Įstaiga gali arba:

45.1. imti pagrįstą mokestį, atsižvelgdama į informacijos teikimo arba pranešimų ar veiksmų, kurių prašoma, administracine išlaidas; arba

45.2. atsisakyti imtis veiksmų pagal prašymą.

46. Duomenų subjektas turi teisę reikalauti, kad Įstaiga ar kitos trečiosios šalys nepagrįstai nedelsdami ištrintų su juo susijusius asmens duomenis, o Įstaiga ar kita trečioji šalis privalo tokį prašymą tenkinti, išskyrus Bendrajame duomenų apsaugos reglamente Nr. 2016/679 (ES) nustatytas išimtis.

47. Informacija apie duomenų subjektus neturėtų būti atskleista kitoms įmonėms, įstaigoms ar organizacijoms, taip pat tretiesiems asmenims, kurie nėra Įstaigos darbuotojai ar su Įstaiga dirbantys ar jos vardu veikiantys asmenys, išskyrus atvejus, kai tai yra teisiškai pagrįstas reikalavimas, kai yra aiškus ar numanomas duomenų subjekto sutikimas arba kai informacija yra viešai prieinama.

XII. ASMENS DUOMENŲ KLASIFIKAVIMAS

48. Įstaiga savo veikloje turi ir tvarko trijų kategorijų asmens duomenis, kuriems taikoma ši politika:

48.1. organizacinė informacija – viešai prieinama informacija apie Įstaigą ir kitus juridinius asmenis bei tam tikra konfidenciali informacija;

48.2. asmens duomenys – informacija, susijusi su identifikuojamais fiziniais asmenimis (duomenų subjektais): darbo ieškančių ir siekiančių įsidarbinti asmenų, esamų ir buvusių darbuotojų, praktikantų, tiekėjų ir kitų duomenų subjektų duomenys. Asmens duomenys, kuriuos

surenka ir tvarko Įstaiga, gali būti įvairūs: asmeniniai duomenys, asmeniniai kontaktiniai duomenys, kvalifikacijos duomenys, finansiniai duomenys, asmens tapatybės duomenys, duomenys, susiję su vykdomu darbu, duomenys apie sveikatą, ir pan.

48.3. jautrūs (specialiosios kategorijos) asmens duomenys – asmeniniai duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėje sąjungoje, taip pat genetiniai, biometriniai duomenys, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenis arba duomenis apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją. Bet kokie jautrūs asmens duomenys turėtų būti griežtai kontroliuojami pagal šią politiką. Įstaiga renka ir apdoroja šiuos jautrius asmens duomenis:

48.3.1. etninę kilmę (išskirtinai tuo atveju, kai tokią informaciją gyvenimo aprašymuose nurodo, pavyzdžiui, siekiantys įsidarbinti asmenys);

48.3.2. duomenis apie sveikatą.

49. Tais atvejais, kai Įstaiga tvarko jautrius asmens duomenis, Įstaiga privalo reikalauti aiškaus duomenų subjekto sutikimo dėl šių duomenų tvarkymo, išskyrus atvejus, kai Įstaiga šiuos duomenis tvarko teisės aktų nustatytais pagrindais. Bet koks toks asmens sutikimas turės aiškiai nustatyti, kokie duomenys yra tvarkomi, kodėl jie yra tvarkomi ir kam jie gali būti perduoti.

XIII. ASMENS DUOMENŲ PAŽEIDIMAS

50. Darbuotojai privalo nedelsiant pranešti apie realius arba galimus asmens duomenų saugojimo pažeidimų atvejus. Tai leidžia Įstaigai:

50.1. ištirti realias ar galimas grėsmes ir, prireikus, imtis atitinkamų veiksmų;

50.2. registruoti tam tikrus pažeidimus;

50.3. įvertinus aplinkybes, pranešti apie realius ar galimus pažeidimus Valstybinei duomenų apsaugos inspekcijai ir, priklausomai nuo situacijos, pačiam duomenų subjektui, kurių duomenims galėjo būti padaryta žala.

51. Jeigu Įstaigos darbuotojai ar kiti Įstaigos vardu veikiantys asmenys gauna bet kokią informaciją apie galimą ar realų incidentą, kurio metu gali būti pažeisti asmens duomenys, įskaitant bet kokią avarinę situaciją (pavyzdžiui, gaisrą, potvynį, nelaimingą atsitikimą ir kt.), jie nedelsdami apie tai turi pranešti Įstaigos direktoriui, tam, kad galima būtų užtikrinti incidentų tyrimą, pranešimą apie tai kompetentingoms valstybinėms institucijoms ir imtasi konkrečių prevencinių veiksmų, siekiant užtikrinti asmens duomenų saugumą.

52. Asmens duomenų pažeidimo atveju Įstaiga turi įvertinti pažeidimo aplinkybes, įskaitant tai, ar asmens duomenys buvo apsaugoti tinkamomis techninėmis saugumo priemonėmis, galimas pažeidimo pasekmes bei poveikį duomenų subjektui, ir nuspręsti, ar apie pažeidimą pranešti Valstybinei duomenų apsaugos inspekcijai. Įstaiga nepagrįstai nedelsdama ir, jei įmanoma, praėjus ne daugiau kaip per 72 (septyniasdešimt dviem) valandoms nuo tada, kai ji sužinojo apie asmens duomenų saugumo pažeidimą, praneša Valstybinei duomenų apsaugos inspekcijai šiais atvejais:

52.1. kai asmens duomenys atsitiktinai prarandami ar neteisėtai atskleidžiami tretiesiems asmenims dideliu mastu (mažiausiai dešimties duomenų subjektų);

52.2. kai buvo nustatyta neteisėta prieiga prie didelės apimties duomenų (mažiausiai dešimties duomenų subjektų);

52.3. kai yra įvykdoma vagystė ar kita nusikalstama veikla, kurios metu prarandami ar sunaikinami asmens duomenys (bent dešimties duomenų subjektų);

52.4. kai yra įvykdomos kibernetinės atakos, nukreiptos į Įstaigos IT sistemas (kompiuterius, įrangą, serverius, internetinę svetainę, kompiuterines programas, elektroninius laiškus ir kt.);

52.5. kai yra nuolatiniai ir nepertraukiami pažeidimai, kurie neigiamai veikia asmens duomenų saugumą, o Įstaigos taikomos apsaugos priemonės nepašalina grėsmės priežasčių;

52.6. bet kokia avarinė situacija ar incidentas (įskaitant gaisrą, potvynį, nelaimingą atsitikimą ir kt.), dėl kurio sunaikinami arba prarandami didelio masto duomenys (mažiausiai dešimties duomenų subjektų).

53. Kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms, Įstaiga nepagrįstai nedelsdama praneša apie asmens duomenų saugumo pažeidimą duomenų subjektui, išskyrus atvejus, kai Įstaiga įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems asmens duomenų saugumo pažeidimas turėjo poveikio arba Įstaiga vėliau ėmėsi priemonių, kuriomis užtikrino, kad nebegalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms.

XIV. BAIGIAMOSIOS NUOSTATOS

54. Įstaiga savo veikloje turi ir naudoja visas reikalingas priemones ir procedūras, užtikrinančias šios politikos laikymąsi ir tinkamą asmens duomenų apsaugą.

55. Visi nauji darbuotojai turėtų būti supažindinti su šia politika ir vykdomais veiksmais duomenų apsaugos srityje, turėtų būti apmokyti, kaip jie turėtų saugoti ir tvarkyti asmens duomenis.

56. Darbuotojams turėtų būti reguliariai rengiami instruktavimai (mokymai) ir konsultacijos dėl asmens duomenų tvarkymo ir saugojimo.

57. Įstaiga kasmet turi tikrinti šią savo politiką ir kitas procedūras.