PATVIRTINTA
Kauno lopšelio-darželio „Vaivorykštė“
direktoriaus 2023 m. kovo 29 d.
įsakymu Nr. V-51

KAUNO LOPŠELIO-DARŽELIO „VAIVORYKŠTĖ“ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pašalinimo ir pranešimo apie juos Kauno lopšelyje-darželyje „Vaivorykštė (toliau – Darželis) tvarką.

2. Aprašas parengtas vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – BDAR).

3. Apraše vartojamos sąvokos:

3.1. **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.

3.2. **Neįgaliotas asmuo** – asmuo, neturintis teisės prieiti prie Darželio turimų asmens duomenų.

4. Kitos Apraše vartojamos sąvokos atitinka BDAR apibrėžtas sąvokas.

5. Galimi šie asmens duomenų saugumo pažeidimai:

5.1. konfidencialumo pažeidimas – neleistinas arba netyčinis asmens duomenų atskleidimas arba prieigos prie jų suteikimas;

5.2. vientisumo pažeidimas – neleistinas arba netyčinis asmens duomenų pakeitimas;

5.3. prieinamumo pažeidimas – neleistinas arba netyčinis prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas.

6. Atsižvelgiant į aplinkybes, saugumo pažeidimas vienu metu gali būti susijęs su asmens duomenų konfidencialumu, vientisumu ir prieinamumu, taip pat su bet kokiu jų deriniu.

7. Asmens duomenų saugumo pažeidimas gali įvykti dėl šių priežasčių:

7.1. žmogiškoji klaida (pvz., asmens duomenys persiųsti ne tam adresatui, kuriam jie buvo skirti; ne saugojimui skirtoje vietoje palikti dokumentai, kuriuose yra asmens duomenų; pamesti

nešiojamieji ar mobilieji įrenginiai (telefonas, nešiojamasis kompiuteris, išorinės duomenų laikmenos), kuriuose saugomi asmens duomenys, ir kt.);

7.2. vagystė (pvz., pavogti nešiojamieji ar mobilieji įrenginiai, kuriuose saugomi asmens duomenys; pavogtos neautomatiniu būdu susistemintos bylos, kuriose yra asmens duomenų, ir kt.);

7.3. kibernetinė ataka (pvz., duomenų bazėje ar informacinėje sistemoje esantys asmens duomenys užšifruojami, naudojant išpirkos reikalaujančią programą; internete paskelbiami informacinių sistemų naudotojų vardai ir slaptažodžiai ir kt.);

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

7.5. įrenginių ar programinės įrangos gedimas, saugos sistemos spragos (pvz., energijos tiekimo nutrūkimas, dėl kurio negalima prieiga prie asmens duomenų; programos kodo, kuriuo kontroliuojamas prieigos teisių suteikimas informacinių sistemų naudotojams, klaida ir kt.);

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

8. Asmens duomenų saugumo pažeidimas, galintis kelti pavojų asmenų teisėms ir laisvėms yra toks, dėl kurio, laiku nesiėmus tinkamų priemonių, fiziniai asmenys gali patirti kūno sužalojimą, materialinę ar nematerialinę žalą (pvz., asmuo gali patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, pakenkta jo reputacijai, prarastas duomenų, kurie laikomi profesine paslaptimi, konfidencialumas ir kt.).

9. Aprašu siekiama užtikrinti, kad Darželio darbuotojai sugebėtų laiku nustatyti galimus asmens duomenų saugumo pažeidimus ir suprastų, kokie veiksmai privalo būti atlikti valdant juos (reikalavimų pranešti apie asmens duomenų saugumo pažeidimą vykdymo schema pateikiama Aprašo 1 priede).

10. Aprašo privalo laikytis visi Darželio darbuotojai, kurie tvarko asmens duomenis arba eidami savo pareigas juos sužino.

11. Aprašo rekomenduojama laikytis juridiniams asmenims, esantiems Darželio duomenų tvarkytojams (toliau – duomenų tvarkytojai), kuriems pagal BDAR straipsnio 2 dalį yra nustatyta prievolė pranešti Darželiui apie kiekvieną asmens duomenų saugumo pažeidimą.

II SKYRIUS
PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

12. Darželio darbuotojas, nustatęs galimą asmens duomenų saugumo pažeidimą arba kai informacija apie galimą saugumo pažeidimą gaunama iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio:

12.1. nedelsdamas, bet ne vėliau kaip per 1 darbo valandą nuo pažeidimo paaiškėjimo momento, žodžiu (tiesiogiai ar telefonu) arba elektroniniu paštu informuoja tiesioginį vadovą ir (arba) Darželio administracijos duomenų apsaugos pareigūną (toliau – duomenų apsaugos pareigūnas);

12.2. užpildo Pranešimą apie asmens duomenų saugumo pažeidimą (Aprašo 2 priedas) ir nedelsdamas, bet ne vėliau kaip per 2 darbo valandas nuo saugumo pažeidimo paaiškėjimo momento, perduoda jį duomenų apsaugos pareigūnui;

12.3. jei įmanoma, imasi priemonių pašalinti saugumo pažeidimą ir (ar) priemonių sumažinti jo sukeltas neigiamas pasekmes.

13. Darželio duomenų tvarkytojas, nustatęs galimą asmens duomenų saugumo pažeidimą, nedelsdamas, bet ne vėliau kaip per 24 valandas nuo pažeidimo paaiškėjimo momento, apie tai praneša Darželiui, pateikdamas užpildytą Pranešimą apie asmens duomenų saugumo pažeidimą (Aprašo 2 priedas).

14. Tuo atveju, jei terminas nuo momento, kai duomenų tvarkytojui tapo žinoma apie saugumo pažeidimą, iki pranešimo Darželiui yra ilgesnis nei 24 valandos, duomenų tvarkytojas kartu su pranešimu pateikia Darželiui paaiškinimą dėl uždelsto informacijos pateikimo.

15. Duomenų tvarkytojas pateikia visą Darželio prašomą informaciją, susijusią su saugumo pažeidimu ir jo tyrimu, per 13 punkte nurodytą laiką.

III SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS IR PAŠALINIMAS

16. Duomenų apsaugos pareigūnas, gavęs Darželio darbuotojo ar duomenų tvarkytojo pateiktą pranešimą apie asmens duomenų saugumo pažeidimą:

16.1. nedelsdamas nagrinėja pranešime nurodytas aplinkybes;

16.2. jei saugumo pažeidimas yra susijęs su elektroninės informacijos saugos incidentu, pasitelkia Darželio ar duomenų tvarkytojo informacinių technologijų specialistus, informacinių sistemų saugos įgaliotinį;

16.3. įvertina, ar padarytas asmens duomenų saugumo pažeidimas;

16.4. jei asmens duomenų saugumo pažeidimas padarytas, nustato pažeidimo pobūdį, priežastis, asmens duomenų kategorijas, jų pobūdį ir kiekį, duomenų subjektų kategorijas ir jų kiekį, įvertina padarytą žalą fiziniams asmenims bei tikėtinas pažeidimo pasekmes;

16.5. įvertina, kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas saugumo pažeidimas;

16.6. nustato, ar apie saugumo pažeidimą būtina pranešti Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI);

16.7. nustato, ar apie saugumo pažeidimą būtina pranešti duomenų subjektams.

17. Atliekant asmens duomenų saugumo pažeidimo tyrimą ir siekiant nustatyti, ar pažeidimas iš tikrųjų įvyko, esamos situacijos įrodymai privalo būti fiksuojami dokumentuose ir užtikrinamas jų atsekamumas.

18. Jei nustatomas asmens duomenų saugumo pažeidimas, duomenų apsaugos pareigūnas papildomai įvertina pažeidimo keliamos rizikos duomenų subjektų teisėms ir laisvėms lygį.

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

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

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

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

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

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

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

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

21. Duomenų apsaugos pareigūnas, atlikęs asmens duomenų saugumo pažeidimo tyrimą, užpildo Asmens duomenų saugumo pažeidimo tyrimo ataskaitą (Aprašo 3 priedas).

22. Saugumo pažeidimo tyrimo ataskaita yra pateikiama Darželio Direktoriui (toliau – Direktorius).

23. Atsižvelgiant į saugumo pažeidimo tyrimo ataskaitą, Direktorius, jei reikia, tvirtina priemonių planą, kuriame numatomas būtinų techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl saugumo pažeidimo pašalinimo, paskiria Duomenų apsaugos pareigūną ir nustato priemonių įgyvendinimo terminus.

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

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

26. Priemonių plane turi būti numatyti veiksmai, skirti ne vien esamo saugumo pažeidimo priežasčiai pašalinti, pavojui fizinių asmenų teisėms ir laisvėms sumažinti ar pašalinti, bet taip pat skirti neleisti pasikartoti pažeidimui. Būtina atsižvelgti į trūkumus ir duomenų tvarkymo silpnąsias vietas, kurios buvo išnaudotos įvykdant saugumo pažeidimą, ir imtis priemonių tiems trūkumams pašalinti.

IV SKYRIUS
PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ PRIEŽIŪROS INSTITUCIJAI

27. Tyrimo metu nustačius, kad asmens duomenų saugumo pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, Duomenų apsaugos pareigūnas nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai tapo žinoma apie pažeidimą, apie tai informuoja VDAI.

28. VDAI informuojama užpildant VDAI direktoriaus įsakymu patvirtintos galiojančios formos pranešimą apie asmens duomenų saugumo pažeidimą.

29. Jeigu įvertinus riziką abejojama, ar asmens duomenų saugumo pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, Duomenų apsaugos pareigūnas kartu su Direktoriumi sprendžia, ar apie pažeidimą turėtų būti pranešta VDAI.

30. Jeigu įvertinus riziką nustatoma, kad tuo metu apie saugumo pažeidimą VDAI pranešti nereikia, bet po kurio laiko situacija gali pasikeisti, tada saugumo pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo (pvz., pamesta USB atmintinė, kurioje saugomi asmens duomenys, užšifruoti taikant pažangų algoritmą. Jeigu yra atsarginės duomenų kopijos ir nėra pavojaus šifro saugumui, apie tokį saugumo pažeidimą pranešti VDAI

nereikia, tačiau jei vėliau paaiškėja, kad gali kilti pavojus šifro saugumui, pažeidimo keliamas pavojus bus vertinamas iš naujo ir apie tokį pažeidimą reikės pranešti VDAI).

31. Tuo atveju kai, priklausomai nuo pažeidimo pobūdžio, būtina atlikti išsamesnį tyrimą, nustatyti visus svarbius faktus, susijusius su pažeidimu, ir per 72 valandas dėl objektyvių priežasčių nėra įmanoma ištirti padarytą pažeidimą, informacija VDAI teikiama etapais, nurodant vėlavimo priežastis. Apie informacijos teikimą etapais VDAI informuojama teikiant pirminį pranešimą.

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

33. Tuo atveju, kai yra įtariama, kad asmens duomenų saugumo pažeidimas turi nusikalstamos veikos požymių, informacija apie galimą nusikalstamą veiką pateikiama atitinkamoms valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą.

V SKYRIUS
PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ DUOMENŲ SUBJEKTUI

34. Tyrimo metu nustačius, kad dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, duomenų apsaugos pareigūnas nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo to laiko, kai buvo sužinota apie pažeidimą, praneša apie tai duomenų subjektui, kurio teisėms ir laisvėms gali kilti didelis pavojus.

35. Duomenų subjektas informuojamas siunčiant jam pranešimą paštu, elektroniniu paštu, telefonu, trumpąja žinute (SMS) ar kitu būdu.

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

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

36.2. priemonių, kurių ėmėsi Darželis, kad būtų pašalintas saugumo pažeidimas;

36.3. Duomenų apsaugos pareigūno arba kito atsakingo asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys;

36.4. kita reikšminga informacija, susijusi su pažeidimu, kuri, Duomenų apsaugos pareigūno manymu, turėtų būti pateikta duomenų subjektui, pvz., patarimai, kaip apsisaugoti nuo galimų neigiamų pažeidimo pasekmių.

37. Pranešimo apie asmens duomenų saugumo pažeidimą duomenų subjektams teikti nereikia jeigu:

37.1. Darželis įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems pažeidimas turėjo poveikio, visų pirma tos priemonės, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su duomenimis, jie būtų nesuprantami (pvz., asmens duomenų šifravimo priemonės);

37.2. iš karto po pažeidimo Darželis ėmėsi priemonių, kuriomis užtikrinama, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms;

37.3. tiesioginio pranešimo duomenų subjektui pateikimas pareikalautų neproporcingai didelių pastangų, pvz., jei jų kontaktiniai duomenys buvo prarasti dėl pažeidimo arba iš pradžių nebuvo žinomi. Tokiu atveju apie pažeidimą viešai paskelbiama Darželio interneto svetainėje, spaudoje, pasitelkiami ne vienas, o keli informavimo būdai arba taikomos panašios priemonės, kuriomis duomenų subjektai būtų efektyviai informuojami (pvz., vien tik pranešimas interneto svetainėje nėra efektyvi informavimo priemonė).

38. Jeigu įvertinus riziką nustatoma, kad tuo metu apie saugumo pažeidimą duomenų subjektams pranešti nereikia, bet po kurio laiko situacija gali pasikeisti, tada pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo (pvz., įvykdoma kibernetinė ataka, naudojant išpirkos reikalaujančią programą, ir duomenų bazėje esantys asmens duomenys užšifruojami. Jei atlikus tyrimą, paaiškėja, kad vienintelė išpirkos reikalaujančios programos užduotis buvo užšifruoti asmens duomenis ir jokio kito kenksmingo poveikio duomenų bazei nėra, apie saugumo pažeidimą reikės pranešti tik VDAI, tačiau jei vėliau paaiškėja, kad prarastas ne tik duomenų prieinamumas, bet ir konfidencialumas, saugumo pažeidimo keliamas pavojus bus vertinamas iš naujo bei sprendžiama, ar atsižvelgiant į tikėtinas saugumo pažeidimo pasekmes reikia apie jį pranešti duomenų subjektams).

39. Tam tikromis aplinkybėmis, kai tai yra pagrįsta, Darželis pasitaręs su teisėsaugos institucijomis ir atsižvelgdama į teisėtus teisėsaugos interesus, gali atidėti asmenų, kuriems pažeidimas turi poveikio, informavimą apie saugumo pažeidimą iki to laiko, kai tai netrukdys saugumo pažeidimo tyrimams.

VI SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

40. Visi asmens duomenų saugumo pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, registruojami Duomenų saugumo pažeidimų žurnale (Aprašo 4 priedas).

41. Informacija apie pažeidimą įvedama nedelsiant, kai tik nustatomas pažeidimo faktas ir įvertinama rizika, bet ne vėliau kaip per 5 darbo dienas.

42. Duomenų saugumo pažeidimų žurnale nurodoma:

42.1. pažeidimo detalės ir tikėtinos pažeidimo pasekmės ir pavojus duomenų subjekto teisėms ir laisvėms (pažeidimo data, pažeidimo pobūdis, priežastys, aplinkybės, iš kur ir kokiu būdu buvo

sužinota apie pažeidimą, asmens duomenų, kurių saugumas pažeistas, kategorijos ir apytikslis skaičius, duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius);

42.2. priemonės, kurių buvo imtasi, kad būtų pašalintas pažeidimas, įskaitant priemones galimoms neigiamoms pažeidimo pasekmėms sumažinti;

42.3. informacija apie pranešimą VDAI apie asmens duomenų saugumo pažeidimą:

42.3.1. jei apie asmens duomenų saugumo pažeidimą nebuvo pranešta VDAI, nurodomi tokio sprendimo motyvai;

42.3.2. jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti VDAI, nurodomos tokio vėlavimo priežastys;

42.4. informacija apie pranešimą duomenų subjektui (subjektams) apie asmens duomenų saugumo pažeidimą:

42.4.1. jei apie asmens duomenų saugumo pažeidimą nebuvo pranešta duomenų subjektui (subjektams), nurodomi tokio sprendimo motyvai;

42.4.2. jei apie asmens duomenų saugumo pažeidimą buvo pranešta duomenų subjektui (subjektams), nurodoma pranešimo (pranešimų) data (datos) ir būdas (būdai);

42.5. kita reikšminga informacija, susijusi su asmens duomenų saugumo pažeidimu.

43. Duomenų saugumo pažeidimų žurnalas yra tvarkomas elektronine forma ir saugomas pagal patvirtintą Darželio dokumentacijos planą.

44. Už Duomenų saugumo pažeidimų žurnalo tvarkymą ir saugojimą atsakingas Duomenų apsaugos pareigūnas.

VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

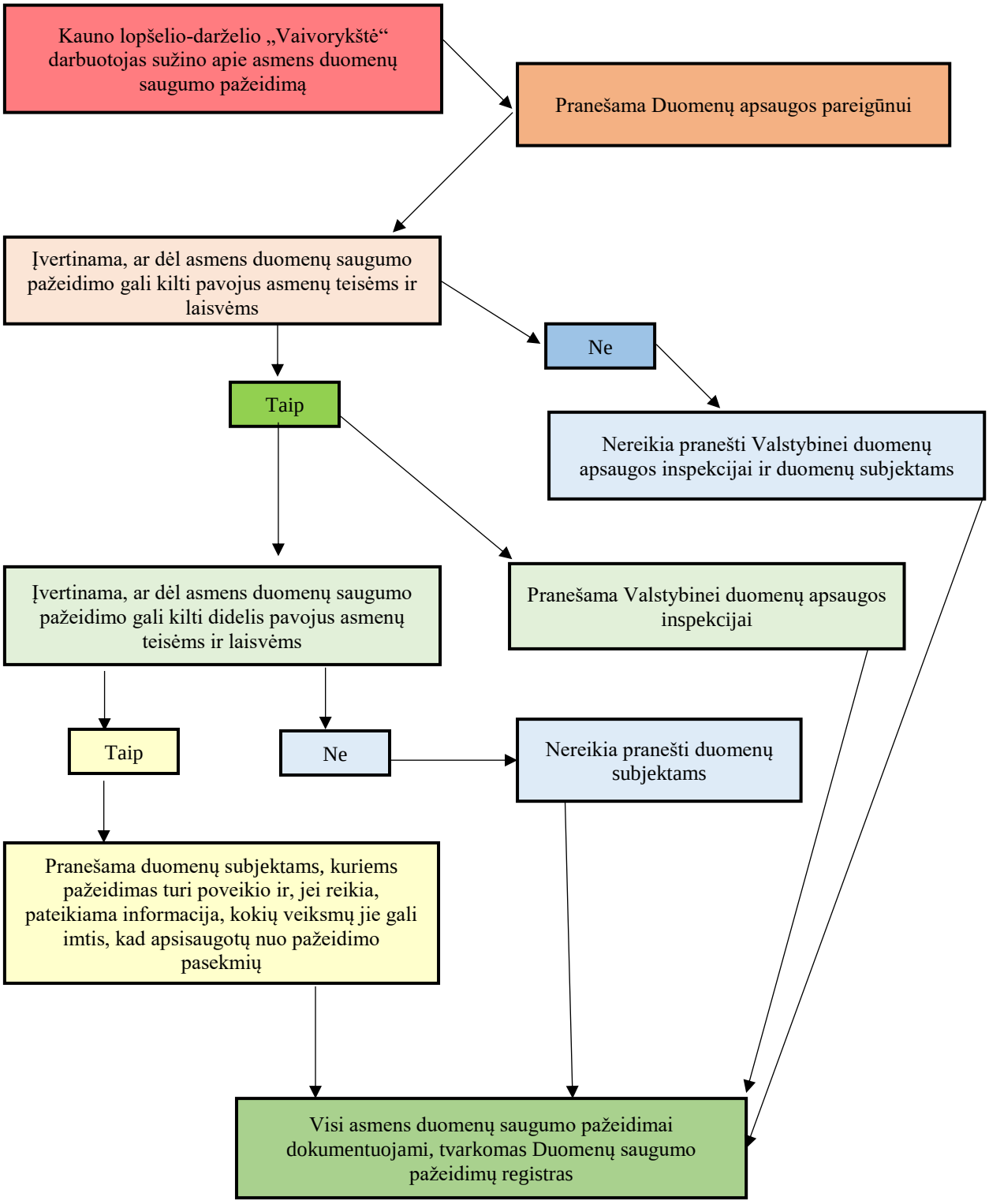
45. Darželio darbuotojai su Aprašu ir jo pakeitimais supažindinami elektroninėmis dokumentų valdymo sistemos priemonėmis.

46. Darželio darbuotojai, pažeidę Aprašo reikalavimus, atsako teisės aktų nustatyta tvarka.

_____

Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo
1 priedas

REIKALAVIMŲ PRANEŠTI APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ VYKDYMO SCHEMA



_____

Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo
2 priedas

KAUNO LOPŠELIS-DARŽELIS „VAIVORYKŠTĖ“

_____
(pareigų pavadinimas)

_____
(vardas, pavardė)

PRANEŠIMAS
APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____ Nr. _____
(data)

Kaunas

Informuoju apie asmens duomenų saugumo pažeidimą, pateikdamas turimą informaciją:

1. Asmens duomenų saugumo pažeidimo nustatymo data, valanda ir vieta:

_____
_____
_____

2. Asmens duomenų saugumo pažeidimo padarymo data, laikas ir vieta:

_____
_____
_____

3. Asmens duomenų saugumo pažeidimo esmė ir aplinkybės:

_____
_____
_____
_____
_____

4. Duomenų subjektų kategorijos (pvz., darbuotojai, asmenys, pateikę prašymus, skundus ir pa.) ir jų skaičius (jei žinoma)).

_____
_____
_____

5. Asmens duomenų kategorijos, susijusios su asmens duomenų saugumo pažeidimu:

5.1. Asmens duomenys:

Vardas	
Pavardė	

Asmens kodas	
Adresas	
Telefono numeris	
Elektroninio pašto adresas	
Banko sąskaitos numeris	
Banko kortelės numeris	
Prisijungimo duomenys (vartotojo vardas, slaptažodis)	
Asmens dokumento (-ų) duomenys	
Duomenys apie apkaltinamuosius nuosprendžius ir nuskalstamas veikas	
Kiti duomenys	

5.2. Specialių kategorijų asmens duomenys:

Duomenys, susiję su asmens sveikata	
Biometriniai duomenys	
Duomenys, susiję su asmens politinėmis pažiūromis, religiniais, filosofiniais įsitikinimais	
Duomenys, susiję su asmens naryste profesinėse sąjungose	
Duomenys, susiję su asmens rasine ar etine kilme	
Duomenys, susiję su asmens lytiniu gyvenimu ar lytine orientacija	

7. Kokių veiksmų (priemonių) buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą (pvz., pakeisti prisijungimo prie informacinės sistemos slaptažodžiai, panaudotos atsarginės kopijos, siekiant atkurti prarastus ar sugadintus duomenis, atnaujinta programinė įranga, surinkti ne saugojimo vietoje palikti dokumentai su asmens duomenimis ir kt.):

_____

_____

_____

_____

_____

_____	_____	_____
(pareigos)	(parašas)	(vardas ir pavardė)

Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo
3 priedas

KAUNO LOPŠELIS-DARŽELIS „VAIVORYKŠTĖ“

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMO ATASKAITA

_____ Nr. _____
(data)

1. Asmens duomenų saugumo pažeidimo aprašymas

1.1. Asmens duomenų saugumo pažeidimo data ir laikas:

Asmens duomenų saugumo pažeidimo data ☐ laikas ☐

Asmens duomenų saugumo pažeidimo nustatymo data ☐ laikas ☐

1.2. Asmens duomenų saugumo pažeidimo vieta (pažymėti tinkamą (-us) atsakymą (-us):

☐ Informacinė sistema
☐ Duomenų bazė
☐ Tarnybinė stotis
☐ Interneto svetainė
☐ Debesų kompiuterijos paslaugos
☐ Nešiojamieji ar mobilieji įrenginiai
☐ Neautomatiniu būdu susistemintos bylos (archyvas)
☐ Kita (įrašyti):

_____

_____

_____

1.3. Asmens duomenų saugumo pažeidimo pobūdis (pažymėti tinkamą (-us) atsakymą (-us):

☐ Konfidencialumo pažeidimas (neautorizuota prieiga ar atskleidimas)
☐ Vientisumo pažeidimas (neautorizuotas asmens duomenų pakeitimas)
☐ Prieinamumo pažeidimas (asmens duomenų praradimas, sunaikinimas)

1.4. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-us) atsakymą (-us) ir aprašyti):

☐ Asmens tapatybę patvirtinantys duomenys (vardas, pavardė, gimimo data, lytis ir kt.):

_____

_____

_____

☐ Asmens identifikaciniai ar prisijungimo duomenys (asmens kodas, mokėtojo kodas, slaptažodžiai ir kt.):

_____

_____

_____

☐ Asmens kontaktiniai duomenys (gyvenamosios vietos adresas, telefono numeris, elektroninio pašto adresas ir kt.):

☐ Specialių kategorijų asmens duomenys (duomenys, susiję su asmens sveikata, genetiniai duomenys, biometriniai duomenys, duomenys, susiję su asmens rasine ar etnine kilme, duomenys, susiję su asmens politinėmis pažiūromis, religiniais, filosofiniais įsitikinimais ar naryste profesinėse sąjungose, duomenys, susiję su asmens lytiniu gyvenimu ir lytine orientacija ir kt.):

☐ Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:

☐ Kiti asmens duomenys:

1.5. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius: ☐

1.6. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (Kauno miesto savivaldybės darbuotojai, asmenys, pateikę prašymus, skundus, asmenys, kuriems teikiamos viešosios ar administracinės paslaugos ir kt.):

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

1.8. Darbuotojas, pranešęs apie asmens duomenų saugumo pažeidimą (vardas, pavardė, Administracijos struktūrinio padalinio, kuriame dirba darbuotojas, pavadinimas, telefono numeris, elektroninio pašto adresas):

1.9. Duomenų tvarkytojas, pranešęs apie asmens duomenų saugumo pažeidimą (pavadinimas, kontaktinio asmens duomenys (vardas, pavardė, telefono numeris, elektroninio pašto adresas):

2. Asmens duomenų saugumo pažeidimo keliamos rizikos duomenų subjektų teisėms ir laisvėms įvertinimas

2.1. Specifiniai fizinių asmenų, kurių asmens duomenų saugumas buvo pažeistas, ypatumai (vaikai, asmenys su negalia ir kt.):

2.2. Galimybė identifikuoti fizinį asmenį (pvz., iki asmens duomenų saugumo pažeidimo asmens duomenys buvo tinkamai užšifruoti, anonimizuoti arba iki saugumo pažeidimo asmens duomenims šifravimas nebuvo taikomas ir kt.):

2.3. Kas gavo prieigą prie asmens duomenų, kurių saugumas pažeistas?

2.4. Ar buvo kokių kitų įvykių ar aplinkybių, turėjusių poveikį asmens duomenų saugumo pažeidimui padaryti?

2.5. Kokia žala padaryta fiziniams asmenims (duomenų subjektams)?

2.6. Galimos asmens duomenų saugumo pažeidimo pasekmės:

2.6.1. Konfidencialumo pažeidimo atveju (pažymėti tinkamą (-us) atsakymą (-us):

☐ Asmens duomenų išplitimas ir duomenų subjekto kontrolės praradimas savo asmens duomenų atžvilgiu (pvz., asmens duomenys išplito internete)

☐ Skirtingos informacijos susiejimas (pvz., gyvenamosios vietos adreso susiejimas su asmens buvimo vieta realiu laiku)

☐ Galimas panaudojimas kitais nei nustatytais ar neteisėtais tikslais (pvz., komerciniais tikslais, asmens tapatybės pasisavinimo tikslu, informacijos panaudojimo prieš asmenį tikslu)

☐ Kita:

2.6.2. Vientisumo pažeidimo atveju (pažymėti tinkamą (-us) atsakymą (-us):

☐ Pakeitimas į neteisingus duomenis, dėl ko asmuo gali netekti galimybės naudotis paslaugomis

☐ Pakeitimas į kitus duomenis, kad asmens duomenų tvarkymas būtų nukreiptas tam tikra linkme (pvz., pavogta asmens tapatybė susiejant vieno asmens identifikuojančius duomenis su kito asmens biometriniais duomenimis)

☐ Kita:

2.6.3. Prieinamumo pažeidimo atveju (pažymėti tinkamą (-us) atsakymą (-us):

☐ Dėl asmens duomenų trūkumo negalima teikti paslaugų (pvz., administracinių procesų sutrikdymas, dėl ko negalima prieiti prie tvarkomų asmens duomenų ir įgyvendinti duomenų subjekto teisę susipažinti su jo tvarkomais asmens duomenimis)

☐ Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamos paslaugos (pvz., tam tikra informacija iš informacinės sistemos išnyko, dėl ko negalima tinkamai suteikti administracinės paslaugos)

☐ Kita:

2.7. Asmens duomenų saugumo pažeidimo sukeltos rizikos duomenų subjektų teisėms ir laisvėms lygis:

☐ Žema rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo nėra pavojaus fizinių asmenų teisėms ir laisvėms)

☐ Vidutinė rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo yra ar gali kilti pavojus fizinių asmenų teisėms ir laisvėms)

☐ Didelė rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo yra ar gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms)

2.8. Kokių veiksmų ar priemonių buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą?

2.9. Kokios taikytos priemonės, siekiant sumažinti neigiamą poveikį duomenų subjektams?

2.10. Kokios techninės priemonės buvo taikomos asmens duomenų saugumo pažeidimo paveiktiems asmens duomenims, užtikrinant, kad asmens duomenys nebūtų prieinami neįgaliotiems asmenims?

2.11. Techninės ir (ar) organizacinės saugumo priemonės, kurios įgyvendintos dėl asmens duomenų saugumo pažeidimo, taip pat siekiant, kad pažeidimas nepasikartotų:

2.12. Techninės ir (ar) organizacinės saugumo priemonės, kurios ketinamos įgyvendinti dėl asmens duomenų saugumo pažeidimo, įskaitant ir priemones sumažinti asmens duomenų saugumo pažeidimo pasekmes:

3. Pranešimų apie asmens duomenų saugumo pažeidimą pateikimas

3.1. Ar pranešta Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI) apie asmens duomenų saugumo pažeidimą?

☐ Taip

☐ Ne (nurodomos nepranešimo VDAI priežastys):

☐ Apie duomenų saugumo pažeidimą pranešta VDAI vėliau nei per 72 valandas (nurodomos vėlavimo pranešti VDAI priežastys):

3.2. Ar pranešta duomenų subjektui apie asmens duomenų saugumo pažeidimą?

☐ Taip

Informuotų duomenų subjektų skaičius

Pranešimo duomenų subjektui turinys:

☐ Ne (nurodomos nepranešimo duomenų subjektui priežastys):

☐ Apie saugumo pažeidimą pranešta viešai (nurodoma kada ir kur paskelbta informacija viešai arba jei taikyta kita priemonė, nurodoma kokia ir kada taikyta):

3.3. Ar pranešta valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, apie asmens duomenų saugumo pažeidimą, galimai turintį nusikalstamos veikos požymių (jeigu taip, nurodoma rašto data ir numeris):

_____	_____	_____
(pareigos)	(parašas)	(vardas ir pavardė)

Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo
4 priedas

KAUNO LOPŠELIO-DARŽELIO „VAIVORYKŠTĖ“

DUOMENŲ SAUGUMO PAŽEIDIMŲ ŽURNALAS

Eil. Nr.	Pažeidimo detalės						Pažeidimo pasekmės				Kokių priemonių buvo imtasi			
	Pažeidimo data, laikas ir vieta	Paveiktų duomenų subjektų kategorijos	Pažeidimo pobūdis, priežastys, aplinkybės	Pažeidimo aprašymas	Informacija, kaip buvo sužinota apie pažeidimą	Paveiktų duomenų kategorijos	Duomenų kiekis	Duomenų jautrumas	Duomenų subjektų kiekis	Galimos pažeidimo pasekmės duomenų subjektams	Informacija, ar visi duomenų subjektai buvo informuoti	Priemonės pažeidimui pašalinti, sumažinti	Informacija, ar pranešta Valstybinei duomenų apsaugos inspekcijai	Pažeidimo nagrinėjimo pabaigos data