PATVIRTINTA
Vilniaus lopšelio – darželio „Prie pasakų parko“
Direktoriaus 2021 m. spalio __ d.
įsakymu Nr. _____

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠAS

Vilnius
2021

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 Vilniaus lopšelio – darželio „Prie pasakų parko“ (toliau – Įstaiga) 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 – Reglamentas (ES) 2016/679).

3. Apraše vartojamos sąvokos atitinka Reglamente (ES) 2016/679 apibrėžtas sąvokas.

4. Galimi šie asmens duomenų saugumo pažeidimai:

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

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

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

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

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

6.1. žmogiškoji klaida (pvz., asmens duomenys persiųsti ne tam adresatui, kuriam jie buvo skirti; ne saugojimui skirtoje vietoje palikti dokumentai, kuriuose yra asmens duomenų; pamesti nešiojami / mobilūs įrenginiai (telefonas, nešiojamas kompiuteris, išorinės duomenų laikmenos), kuriuose saugomi asmens duomenys ir kt.);

6.2. vagystė (pvz., pavogti nešiojami / mobilūs įrenginiai, kuriuose saugomi asmens duomenys; pavogtos neautomatiniu būdu susistemintos bylos, kuriose yra asmens duomenų ir kt.);

6.3. 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.);

6.4. 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.);

6.5. 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.);

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

7. 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.).

8. Šis Aprašas skirtas užtikrinti, kad Įstaigos darbuotojai, dirbantys pagal darbo sutartį (toliau – Įstaigos darbuotojai), sugebėtų laiku nustatyti galimus asmens duomenų saugumo pažeidimus bei suprastų, kokie veiksmai privalo būti atlikti valdant juos.

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

II SKYRIUS
PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

10. Įstaigos darbuotojas, nustatęs galimą asmens duomenų saugumo pažeidimą, arba gavęs informaciją apie galimą saugumo pažeidimą iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio:

10.1. nedelsdamas, bet ne vėliau kaip per 2 darbo valandas nuo asmens duomenų saugumo pažeidimo paaiškėjimo momento, žodžiu (tiesiogiai ar telefonu) arba elektroniniu paštu informuoja tiesioginį vadovą.

10.2. užpildo Pranešimą apie asmens duomenų saugumo pažeidimą (Aprašo 1 priedas) ir nedelsdamas, bet ne vėliau kaip per 2 darbo valandas nuo saugumo pažeidimo paaiškėjimo momento, perduoda jį Įstaigos vadovui.

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

III SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS IR PAŠALINIMAS

11. Įstaigos vadovas, gavęs Įstaigos darbuotojo pranešimą apie asmens duomenų saugumo pažeidimą:

11.1. nedelsdamas nagrinėja pranešime nurodytas aplinkybes;

11.2. konsultuojasi su Valstybinės duomenų apsaugos inspekcijos (toliau – VDAI) duomenų apsaugos pareigūnu;

11.3. jei saugumo pažeidimas yra susijęs su elektroninės informacijos saugos incidentu, pasitelkia Įstaigos ar duomenų tvarkytojo IT specialistus ir informacinių sistemų saugos specialistus;

11.4. įvertina, ar padarytas asmens duomenų saugumo pažeidimas;

11.5. 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;

11.6. įvertina, kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas saugumo pažeidimas (pvz., naudoti atsargines kopijas, siekiant atkirti prarastus ar sugadintus duomenis ar kt.);

11.7. nustato, ar apie saugumo pažeidimą būtina pranešti VDAI;

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

12. Įstaigos darbuotojai, atsakingi už asmens duomenų tvarkymą, pateikia Įstaigos duomenų apsaugos pareigūnui visą jo prašomą informaciją, susijusią su asmens duomenų saugumo pažeidimu ir tyrimu, per jo nurodytą terminą.

13. 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.

14. 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:

14.1. saugumo pažeidimo pobūdis (konfidencialumo, vientisumo ar prieinamumo pažeidimas) – nustatomas saugumo pažeidimo pobūdis, nuo kurio gali priklausyti pavojaus duomenų subjektams dydis;

14.2. 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;

14.3. 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);

14.4. 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;

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

14.6. 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.

15. Įvertinus riziką nustatomas vienas iš trijų rizikos tikimybių lygių – mažas, vidutinis ar didelis rizikos tikimybės lygis.

16. Įstaigos vadovas, atlikęs asmens duomenų saugumo pažeidimo tyrimą, užpildo Asmens duomenų saugumo pažeidimo tyrimo ataskaitą (Aprašo 2 priedas).

17. Atsižvelgiant į Asmens duomenų saugumo pažeidimo tyrimo ataskaitą, Įstaigos direktorius, jei reikia, tvirtina priemonių planą, kuriame numatomas būtinų techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl saugumo pažeidimo pašalinimo, paskiria atsakingus vykdytojus ir nustato priemonių įgyvendinimo terminus.

18. Sprendžiant asmens duomenų saugumo pažeidimo pašalinimo klausimą bei tvirtinant priemonių planą, priklausomai nuo konkrečių pažeidimo aplinkybių pirmiausia būtina atlikti veiksmus, siekiant apriboti ar sustabdyti saugumo incidentą: ištrinti asmens duomenis nuotoliniu būdu iš pamesto ar pavogto nešiojamo / mobilaus įrenginio (telefono, nešiojamo kompiuterio ir kt.); jei asmens duomenys per klaidą išsiunčiami ne tam adresatui, 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.

19. Siekiant apriboti ar sustabdyti asmens duomenų saugumo pažeidimą, būtina kiek įmanoma tiksliau surinkti duomenis ir įrodymus 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.).

20. Priemonių plane turi būti numatytos prevencinės ir kitos priemonės, užtikrinančios, kad pažeidimas nepasikartotų.

IV SKYRIUS
PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ PRIEŽIŪROS INSTITUCIJAI

21. Tyrimo metu nustačius, kad asmens duomenų saugumo pažeidimas buvo, Įstaigos vadovas nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai tapo žinoma apie pažeidimą, apie tai informuoja VDAI, išskyrus atvejus, kai saugumo pažeidimas nekelia pavojaus fizinių asmenų teisėms ir laisvėms.

22. VDAI informuojama Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo, patvirtinto VDAI direktoriaus 2018 m. liepos 27 d. įsakymu Nr. 1T-72(1.12.E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo patvirtinimo“, nustatyta tvarka ir sąlygomis, užpildant Pranešimo apie asmens duomenų saugumo pažeidimo formą, patvirtintą VDAI direktoriaus 2018 m. rugpjūčio 29 d. įsakymu Nr. 1T-82(1.12.E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo“ (toliau – pranešimas).

23. Jeigu įvertinus riziką abejojama, ar asmens duomenų saugumo pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, apie pažeidimą pranešama VDAI.

24. Jeigu įvertinus riziką nustatoma, kad apie saugumo pažeidimą VDAI pranešti nereikia, tačiau po kurio laiko situacija pasikeičia, saugumo pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turi būti vertinamas iš naujo ir, jeigu reikia, pranešama VDAI (pvz., pamesta USB atmintinė, kurioje saugomi užšifruoti asmens duomenys 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 turi būti vertinamas iš naujo ir apie tokį pažeidimą reikia pranešti VDAI).

25. Tuo atveju, kai pagal pažeidimo pobūdį būtina atlikti išsamesnį tyrimą, tačiau per 72 valandas dėl objektyvių priežasčių ištirti padarytą pažeidimą nėra įmanoma, informacija VDAI teikiama etapais, nurodant vėlavimo priežastis. Apie informacijos teikimą etapais VDAI informuojama teikiant pirminį pranešimą.

26. Jeigu pateikus VDAI pranešimą ir atlikus tolesnį tyrimą yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai nebuvo asmens duomenų saugumo pažeidimo, apie tai nedelsiant informuojama VDAI.

27. 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

28. Tyrimo metu nustačius, kad dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, Įstaigos vadovas, 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.

29. Duomenų subjektas informuojamas tiesiogiai, t. y. siunčiant jam pranešimą paštu, elektroniniu paštu, trumpąja žinute (SMS) ar kitu būdu. Pranešimas duomenų subjektui siunčiamas atskirai nuo kitos siunčiamos informacijos, tokios kaip naujienlaiškiai ar standartiniai pranešimai.

30. 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:

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

30.2. priemonių, kurių ėmėsi Įstaigos, kad būtų pašalintas saugumo pažeidimas, įskaitant priemonių galimoms neigiamoms jo pasekmėms sumažinti aprašymas;

30.3. Įstaigos vadovo arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys;

30.4. kita reikšminga informacija, susijusi su pažeidimu, turėtų būti pateikta duomenų subjektui, pvz., patarimai, kaip apsisaugoti nuo galimų neigiamų pažeidimo pasekmių.

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

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

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

32. Jeigu įvertinus riziką nustatoma, kad apie saugumo pažeidimą duomenų subjektui pranešti nereikia, tačiau po kurio laiko situacija pasikeitė, todėl pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo (pvz., įvykdoma kibernetinė ataka, naudojant išpirkos reikalaujančią programą, – 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).

33. Įstaiga, atsižvelgdama į esamas pagrįstas aplinkybes ir teisėtus teisėsaugos institucijų reikalavimus, gali atidėti asmenų, kuriems pažeidimas turi poveikio, informavimą iki to laiko, kol tai netrukdys saugumo pažeidimo tyrimui.

VI SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

34. Visi asmens duomenų saugumo pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, registruojami Asmens duomenų saugumo pažeidimų registravimo žurnale (Aprašo 3 priedas).

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

36. Asmens duomenų saugumo pažeidimų registravimo žurnale nurodoma:

36.1. pažeidimo nustatymo aplinkybės (pažeidimo nustatymo data, laikas, vieta, subjektas, pranešęs apie pažeidimą);

36.2. pažeidimo aplinkybės (pažeidimo data, vieta, pažeidimo pobūdis, priežastys, asmens duomenų, kurių saugumas pažeistas, kategorijos ir apytikslis skaičius, duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius);

36.3. tikėtinos pažeidimo pasekmės ir pavojus duomenų subjekto teisėms ir laisvėms;

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

36.5. informacija apie pranešimą ar nepranešimą VDAI:

36.5.1. jei apie asmens duomenų saugumo pažeidimą buvo nepranešta VDAI, nurodomi tokio sprendimo motyvai; jei apie asmens duomenų saugumo pažeidimą buvo pranešta VDAI, nurodoma pranešimo data ir numeris, taip pat, ar pranešimas teikiamas etapais;

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

36.6. informacija apie pranešimą ar nepranešimą duomenų subjektui (subjektams):

36.6.1. jei apie asmens duomenų saugumo pažeidimą buvo nepranešta duomenų subjektui (subjektams), nurodomi tokio sprendimo motyvai; jei apie asmens duomenų saugumo pažeidimą buvo pranešta duomenų subjektui (subjektams), nurodoma pranešimo (pranešimų) data (datos) ir būdas (būdai);

36.6.2. jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti duomenų subjektui (subjektams), nurodomos tokio vėlavimo priežastys;

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

37. Asmens duomenų saugumo pažeidimų registravimo žurnalas yra tvarkomas ir saugomas pagal patvirtintą Įstaigos dokumentacijos planą.

38. Už Asmens duomenų saugumo pažeidimų registravimo žurnalo tvarkymą ir saugojimą atsakingas Įstaigos vadovas.

VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

39. Įstaigos darbuotojai su šiuo Aprašu bei jo pakeitimais supažindinami dokumentų valdymo sistemos priemonėmis; darbuotojai, kurie neturi prieigos prie dokumentų valdymo sistemos, su Aprašu supažindinami pasirašytinai.

40. Įstaigos darbuotojai, pažeidę šio Aprašo reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.